RING EXTENSIONS WITH IDENTITY ELEMENT

by

Edward F. Card

Submitted in partial fullfillment of the requirements

for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
August, 1994

[redacted]

DALHOUSIE UNIVERSITY

DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTING SCIENCE

The undersigned hereby certify that they have read and recommend to the Faculty of Graduate Studies for acceptance a thesis entitled "RING EXTENSIONS WITH IDENTITY ELEMENT"

by Edward F. Card

in partial fulfillment of the requirements for the degree of Master of Science.

Dated 13 September, 1994

Supervisor: [redacted]

Readers:

DALHOUSIE UNIVERSITY

DATE: Sept 15, 1994

AUTHOR: Edward F. Card

TITLE: Ring Extensions With Identity Element

DEPARTMENT OR SCHOOL: Mathematics, Statistics And Computing Science

DEGREE: M.Sc. CONVOCATION: October YEAR: 1994

[redacted]

Signature of Author

Table of Contents

Abstract

We will consider different methods which extend any given ring to a ring which contains an identity element. Each construction will be examined to determine properties which are retained by the extension if possessed by the original ring.

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Professor Patrick Stewart, for his patience and guidance throught the creation of this thesis.

I would also like to thank my good friends, Dr. Michael Wendt, for his assistance in the area of Category Theory, and Todd Saulnier, for his assistance with the preparation of this manuscript.

I would also like to express my gratitude to my wife, Charlotte, for her love, support and encouragement while I was writing this thesis.

Finally, I would like to acknowledge my children, Ian and Lynn, my parents and other family members for their understanding and support while I was a masters student.

CHAPTER 1

The Characteristic Ring

§1.1 Introduction

In this thesis, we will examine various constructions which have been developed to extend a given ring to a ring with an identity element. One extension which we will examine, which preserves many of the properties of the original ring, is constructed by adjoining an epimorphic image of the ring of the integers to the original ring. For any given ring S, the Z-epimorph used in this construction is called the characteristic ring of S, and is uniquely determined by the additive structure of S. This chapter examines the epimorphs of the ring of integers and develops the notion of the characteristic function.

We begin the next section with a discussion of the structure of Z-epimorphs. First, given that a ring R is a Z-epimorph, it will be shown that it has one of three possible structures. Conversely, it will then be shown that any ring which has one of these three structures is a Z-epimorph. Results of this section are due to [CHEA 72, DICK 84, STOR 68].

The last section of this chapter develops the notion of the characteristic function. This characteristic function is uniquely determined by a given ring S, and associates with S a Z-epimorph, called the characteristic ring of S. Later chapters will use this characteristic ring to construct an extension of S which has an identity and preserves many properties of the original ring S.

§1.2 Epimorphs of the Ring of Integers

This section characterizes the epimorphisms of the ring of integers. As will be seen later, the "characteristic ring" $K(End\, S)$ of any arbitrary ring S will be defined as an epimorphism of the ring of integers. This characteristic ring $K(End\,S)$ may be used to construct an extension of the original ring S which contains an identity element and preserves many of the properties of the original ring S.

In this section, each of the rings we will consider has an identity element, denoted 1. Where ambiguity may arise, the identity of any given ring S will be denoted 1_S. All homomorphisms $g : A \longrightarrow B$ will be assumed to satisfy $g(1_A) = 1_B$. The ring of integers is denoted by Z, the field of rationals by Q, the natural numbers by N and the set of prime integers by P.

Definition 1.2.1 Given any two rings A and B, and a homomorphism $g : A \longrightarrow B$, we say that g is an epimorphism if, for any ring C and homomorphisms $f_1 : B \longrightarrow C$ and $f_2 : B \longrightarrow C$, we have $f_1 = f_2$ if $f_1 \circ g = f_2 \circ g$. In this case, we call B an epimorph of A, or simply an A-epimorph. □

Throughout this section the ring R will denote a Z-epimorph through the epimorphism $f : Z \longrightarrow R$. Of course, f is completely determined by $f(1) = 1_R$.

Definition 1.2.2 Given a ring A, an additive abelian group W is a left A-module if there is a scalar multiplication, $* : A \times W \longrightarrow W$, defined for all a, b in A and for all w, x in W, satisfying:

1. $a * (w + x) = a * w + a * x$
2. $(a + b) * w = a * w + b * w$
3. $(ab) * w = a * (b * w)$
4. $1 * w = w$ in the case where A has an identity.

Right A-modules are defined similarly. W is said to be an A-bimodule if and only if W is both a left and a right A-module and $(a * w) * b = a * (w * b)$. □

It should be noted that any ring S together with its additive operation $+$ is an additive abelian group and therefore may be considered an A-module for some ring A in this way. We first require a lemma concerning modules, followed by a discussion regarding the structure of R.

Lemma 1.2.1 *Let A and K be rings and $g : A \longrightarrow K$ a homomorphism. Then the scalar multiplications $* : A \times K \longrightarrow K$ and $*' : K \times A \longrightarrow K$ defined by $a * k = g(a)k$ and $k *' a = kg(a)$ for any a in A and any k in K, causes K to be an A-bimodule.*

Proof. We note that $g(a)$ is an element of K for all a in A, and that the ring structure of K satisfies the four requirements which make K an A-bimodule, giving our desired result. ■

Definition 1.2.3 Given a ring A, a ring W is called an <u>A-bimodule algebra</u> if W is an A-bimodule and satisfies

$$a * (wx) = (a * w)x = w(a * x) = (wx) * a = w(x * a) = (w * a)x$$

for all $w, x \in W$ and all $a \in A$. □

Corollary 1.2.1 *Every ring K with identity is a Z-bimodule algebra.*

We now consider a given Z-epimorph, R, and determine its structure. Later in this section we will show the converse, that any ring which is of one of three given structures is in fact a Z-epimorph. To begin, we prove the following lemma which shows that every Z-epimorph is commutative.

Lemma 1.2.2 *[DICK 84] R is commutative.*

Proof. Let $R[x]$ be the polynomial ring of R, and recall that $f : Z \longrightarrow R$ is the unique epimorphism from Z to R such that $f(1) = 1_R$. Let I be the ideal of $R[x]$

generated by x^2 and consider $R[x]/I$. For each element a of R we see that $(1-ax)+I$ is the multiplicative inverse of $(1+ax)+I$ since

$$[(1+ax)+I][(1-ax)+I] = (1-a^2x^2)+I = 1+I.$$

For a fixed element b of R we define two ring homomorphisms, as follows:

$$f_1 : R \longrightarrow R[x]/I$$

where $f_1(r) = (1+bx)r(1-bx)+I$, and

$$f_2 : R \longrightarrow R[x]/I$$

where $f_2(r) = r+I$. We see that $f_1 \circ f = f_2 \circ f$, so $f_1 = f_2$ since f is an epimorphism. Thus for all r in R,

$$r+I = (1+bx)r(1-bx)+I = r+bxr-rbx-brbxx+I = r+(br-rb)x+I.$$

Therefore $(br-rb)x$ is an element of I. Since I is generated by x^2, we see that $br-rb=0$, so $br=rb$ proving that R is commutative. ∎

Throughout this chapter, a tensor product over a ring S will be denoted by $\otimes_S$, except in the case where $S=Z$ when the subscript will be omitted. We now consider a tensor product, over Z, of a given Z-epimorph R and any ring K with identity. This tensor product $R \otimes K$ is shown to be a K-epimorph. This result is then used to show that when K is a field either $R \otimes K \simeq K$ or $R \otimes K \simeq 0$.

Lemma 1.2.3 *For any ring K, $R \otimes K$ is a K epimorph.*

Proof. Let $g_1 : R \longrightarrow R \otimes K$ and $g_2 : K \longrightarrow R \otimes K$ be the canonical homomorphisms of R and K into $R \otimes K$, respectively. Consider a ring T and two homomorphisms $h_1, h_2 : R \otimes K \longrightarrow T$ such that $h_1 \circ g_2 = h_2 \circ g_2$. We now look at the resultant diagram, where g is the unique homomorphism of Z into K.

$$\begin{tikzcd}
Z \arrow[r, "f\text{ (epi)}"] \arrow[d, "g"] & \mathrm{R} \arrow[d, "g_1"] & \\
K \arrow[r, "g_2"'] & R \otimes K \arrow[r, shift left, "h_1"] \arrow[r, shift right, "h_2"'] & T
\end{tikzcd}$$

We first note that, for any n in Z,

$$\begin{aligned}
g_1 \circ f(n) &= g_1(n1_R) \\
&= n1_R \otimes 1_K \\
&= 1_R \otimes n1_K \\
&= g_2(n1_K) \\
&= g_2 \circ g(n),
\end{aligned}$$

and so the rectangle commutes (i.e. $g_1 \circ f = g_2 \circ g$).

Since $h_1 \circ g_2 = h_2 \circ g_2$ by assumption, we have

$$h_1(1 \otimes k) = h_2(1 \otimes k)$$

for all k in K. Also, we see that $h_1 \circ g_2 \circ g = h_2 \circ g_2 \circ g$, so that $h_1 \circ g_1 \circ f = h_2 \circ g_1 \circ f$. Since f is an epimorphism we have that $h_1 \circ g_1 = h_2 \circ g_1$, and so

$$h_1(r \otimes 1) = h_2(r \otimes 1)$$

for all r in R.

Thus, for all $r \otimes k$ in $R \otimes K$,

$$\begin{aligned}
h_1(r \otimes k) &= h_1((r \otimes 1)(1 \otimes k)) \\
&= h_1(r \otimes 1)h_1(1 \otimes k) \\
&= h_2(r \otimes 1)h_2(1 \otimes k) \\
&= h_2(r \otimes k),
\end{aligned}$$

and so $h_1 = h_2$. Thus g_2 is an epimorphism. ∎

Lemma 1.2.4 *For any field K either $R \otimes K \simeq K$ or $R \otimes K \simeq 0$.*

Proof. Denote $R \otimes K$ by R_K. We consider the ring

$$N = \begin{pmatrix} R_K & R_K \otimes_K R_K \\ 0 & R_K \end{pmatrix}$$

and note that the diagonal map

$$h : R_K \longrightarrow \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \middle| \; x \in R_K \right\}$$

is an isomorphism. Denote by a the unit

$$\begin{pmatrix} (1 \otimes 1) & (1 \otimes 1) \otimes_K (1 \otimes 1) \\ 0 & (1 \otimes 1) \end{pmatrix}.$$

Note that

$$a^{-1} = \begin{pmatrix} (1 \otimes 1) & (-1 \otimes 1) \otimes_K (1 \otimes 1) \\ 0 & (1 \otimes 1) \end{pmatrix}.$$

For all k in K we have

$$\begin{aligned} & a \begin{pmatrix} 1 \otimes k & 0 \\ 0 & 1 \otimes k \end{pmatrix} a^{-1} \\ &= \begin{pmatrix} (1 \otimes k) & (-1 \otimes k) \otimes_K (1 \otimes 1) + (1 \otimes 1) \otimes_K (1 \otimes k)) \\ 0 & 1 \otimes k \end{pmatrix} \\ &= \begin{pmatrix} 1 \otimes k & 0 \\ 0 & 1 \otimes k \end{pmatrix} \end{aligned}$$

since

$$\begin{aligned}(-1\otimes k)\otimes_K(1\otimes 1) &= (-1\otimes 1)k\otimes_K(1\otimes 1)\\ &= (-1\otimes 1)\otimes_K k(1\otimes 1)\\ &= (-1\otimes 1)\otimes_K(1\otimes k).\end{aligned}$$

Thus the inner automorphism ϕ defined on N, which is determined by a, fixes the image of K in N.

Denote by $g : K \longrightarrow R_K$ the canonical homomorphism (epimorphism) and consider the diagram

$$\begin{tikzcd} K \arrow[r, "g", "epi"'] & R_K \arrow[r, "h"] & \begin{pmatrix} R_K & R_K\otimes_K R_K \\ 0 & R_K \end{pmatrix} \arrow[r, shift left, "\phi"] \arrow[r, shift right, "i"'] & \begin{pmatrix} R_K & R_K\otimes_K R_K \\ 0 & R_K \end{pmatrix} \end{tikzcd}$$

where i is the identity map and ϕ is the inner automorphism determined by a. Since $\phi = i$ on K and g is an epimorphism, we see that $\phi\circ h = i\circ h$. Let r be an element in R_K. Comparing the row 1 column 2 entries of $\phi\circ h(r)$ and $i\circ h(r)$ we see that

$$(-r\otimes_K 1_{R_K}) + (1_{R_K}\otimes_K r) = 0$$

for all r in R_K, so

$$(r\otimes_K 1_{R_K}) = (1_{R_K}\otimes_K r).$$

We now consider R_K as a vector space over K and suppose $dim_K(R_K) > 1$. Then there exists an element x in R_K such that the set $\{1, x\}$ is linearly independent. Thus it follows that $\{x\otimes 1, 1\otimes x\}$ is linearly independent in the K-vector space $R_K\otimes_K R_K$. But this is a contradiction since we have shown $x\otimes 1 = 1\otimes x$. Thus $dim_K(R_K)\le 1$ and so either $R_K\simeq K$ or $R_K\simeq 0$. ■

For results which follow, we require the following lemma which determines the zeros of tensor products. This lemma is stated without proof.

Lemma 1.2.5 *[STEN 75] Let L be a right A-module and M a left A-module. Let $\{y_i \mid i \in I\}$ be a set of generators for M, for some index set I, and let $\{x_i \mid i \in I\}$ be a set of elements of L such that almost all $x_i = 0$. Then $\sum x_i \otimes y_i = 0$ in $L \otimes_A M$ if and only if there exists a finite set $\{u_j \mid j \in J\}$ of elements of L and a set $\{a_{ji} \mid i \in I, j \in J\}$ of elements of A such that*

i) $a_{ji} = 0$ for almost all (j, i);

ii) $\sum a_{ji} y_i = 0$ for each j in J; and

iii) $x_i = \sum u_j a_{ji}$ for each i in I.

Definition 1.2.4 Let S be a ring and $S_1, S_2, \ldots S_k$ be right ideals of S. Then $S_1 \oplus \cdots \oplus S_k$ is a <u>direct sum</u> of right ideals of S if $S_j \cap \sum_{i=1, i\neq j}^{k} S_i = 0$ for all $j = 1, 2, \ldots, k$. □

We will require the following notation in the discussion to follow. Let $t_p(R) = \left\{r \in R \mid p^k r = 0 \text{ for some } k \geq 1\right\}$, for any prime integer p. Let $tR = \oplus_{p \in P} t_p(R)$. Thus $t_p(R)$ and tR are ideals of R. We note that an element r is contained in tR if and only if there exists a positive integer m such that $mr = 0$. In the case where $tR = 0$ we say that R is torsion-free.

Lemma 1.2.6 *Let Y be a subset of the primes of Z, and let $h : R \longrightarrow R \otimes Z[Y^{-1}]$ be the canonical homomorphism. Then $ker\, h = \oplus_{p \in Y} t_p(R)$.*

Proof. Suppose r is an element of $\oplus_{p \in Y} t_p(R)$. Then there exists a positive integer m, whose prime factors belong to Y, such that $mr = 0$. This implies that $mr \otimes 1/m = 0$, so that $r \otimes 1 = h(r) = 0$. Thus r is contained in $ker\, h$.

Suppose r is an element of $ker\, h$. Then $h(r) = r \otimes 1 = 0$. Let M be the set consisting of 1 and the positive integers which are products of primes in Y. Denote the elements of M by $m_1, m_2, m_3, \cdots$ such that $m_i < m_{i+1}$ for all i. We note that $m_1 = 1$. Let $y_i = 1/m_i$. Then $\{y_i\}$ is a set of generators for $Z[Y^{-1}]$ as a left Z-module. Consider the set $\{x_i\}$ where $x_1 = r$ and $x_i = 0$ for all $i > 1$. Thus $0 = r \otimes 1 = \sum_{i=1}^{\infty}(x_i \otimes y_i)$. Hence, by Lemma 1.2.5, there is a set $\{u_j\}$ in R and a set $\{a_{ji}\}$ in Z such that:

1) almost all the $a_{ji} = 0$; thus there exists an integer $\bar{M}$ such that $a_{ji} = 0$ if either $i > \bar{M}$ or $j > \bar{M}$;

2) for each j we have that $\sum_{i=1}^{\infty} a_{ji} y_i = 0$;

3) for each i we have that $x_i = \sum_{j=1}^{\infty} a_{ji} u_j$; that is, $r = \sum_{j=1}^{\infty} a_{j1} u_j$ and $0 = \sum_{j=1}^{\infty} a_{ji} u_j$ for $i > 1$.

Select an integer $k \geq \bar{M}$ such that all prime factors of k are in Y and if $a_{ji} \neq 0$, then $m_i \leq k$.

Consider a function $g : M \to Z[Y^{-1}]$ such that $g(m_i) = k!/m_i$. Note that when $m_i \leq k$ then $g(m_i)$ is an integer. Since $\sum_{i=1}^{\infty} a_{ji}(1/m_i) = 0$ for each j,

$$k! \left(\sum_{i=1}^{\infty} a_{ji}(1/m_i) \right) u_j = 0$$

for each j. Thus $\sum_{i=1}^{\infty} k!(1/m_i) a_{ji} u_j = 0$ and so $\sum_{i=1}^{\infty} g(m_i) a_{ji} u_j = 0$ for all j. Therefore

$$\sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} g(m_i) a_{ji} u_j \right) = 0,$$

so

$$0 = \sum_{i=1}^{\infty} \left(g(m_i) \sum_{j=1}^{\infty} a_{ji} u_i \right) = g(1) r = k! r.$$

Therefore r is contained in $\oplus_{p \in Y} t_p(R)$ and so $ker\, h = \oplus_{p \in Y} t_p(R)$. ∎

For any prime p of Z we can fix $K = Z/(p)$, a field. Hence $R \otimes Z/(p)$ is isomorphic to either $Z/(p)$ or 0. From Lemma 1.2.6 we see that

$$\begin{aligned} R \otimes Z/(p) &= \left\{ \sum_i (r_i \otimes \bar{n}_i) \mid r_i \in R, \bar{n}_i \in Z/(p) \right\} \\ &= \left\{ \sum_i (n_i r_i \otimes 1_K) \mid \bar{n}_i = n_i + (p) \in Z/(p) \right\} \\ &\simeq R/pR. \end{aligned}$$

Hence R/pR is isomorphic to either $Z/(p)$ or 0. It follows that for every prime p in Z, $pR + Z1_R = R$.

We note that for any ideals I and J of Z, if $IR + Z1_R = R = JR + Z1_R$ then

$$IJR + Z1_R = IJR + I1_R + Z1_R = I(JR + Z1_R) + Z1_R = IR + Z1_R = R.$$

So we have that $IR + Z1_R = R$ for all non-zero ideals I of Z since every non-zero ideal of Z is a product of prime ideals.

Corollary 1.2.2 *Let $h : R \longrightarrow R_Q = R \otimes Q$ be the canonical homomorphism. Then $ker\, h = tR$.*

Proof. This follows from Lemma 1.2.6 if we take Y to be the set of all prime numbers. ∎

We now prove one of the two main results of this section, by showing that any Z-epimorph, R, has one of three forms. Later in this section we will show the converse, that any ring which has one of these three forms is a Z-epimorph. Infinite sequences $u_1, u_2, u_3 \ldots$ will be denoted $\langle u_i \rangle$.

Definition 1.2.5 A ring A is *p − divisible* if for each $a \in A$ there is a $b \in A$ such that $a = pb$. □

Lemma 1.2.7 *R has one of the following forms:*

(A) R is isomorphic to Z/I for some ideal I of Z;

(B) R is isomorphic to $D \oplus Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$ where the p_i are primes, the n_i are positive integers, and D is a ring such that $Z \subseteq D \subseteq Q$ which is divisible by the p_i; or

(C) R is isomorphic to a subring of $\prod_{i=1}^{\infty} Z/(p_i^{n_i})$, for some infinite set of primes $\{p_i\}$ and some infinite set of positive integers $\{n_i\}$, consisting of all sequences $\langle u_i \rangle$ where u_i has the form $\bar{a}/\bar{b}$ in $Z/(p_i^{n_i})$ for almost all i, for some element a/b in a ring D where $Z \subseteq D \subseteq Q$ and D is divisible by the primes p_i.

Proof. If we consider the canonical homomorphism $h : R \longrightarrow R \otimes Q = R_Q$, we see that $ker\, h = tR$ and that R/tR is isomorphic to the image of R in R_Q. Since $R_Q \simeq 0$ or Q, we have either:

1) $R = tR$ in the case where $R_Q = 0$, and so the annihilator of 1_R is a non-zero ideal I of Z. Recall that $R = JR + Z1_R$ for all nonzero ideals J of Z. Now, since $IR = 0$, $R = Z1_R \simeq Z/I$ as required; or

2) In the case where $R_Q \simeq Q$ we have that R/tR is isomorphic to a subring of Q. We now check that the epimorphism $f : Z \longrightarrow R$ is injective. If this were not the case there would be a non-zero m in Z such that $m1_R = 0$, so that $m1_R \otimes 1_Q = 0$ in R_Q, in which case $tR_Q \neq 0$ contradicting $R_Q \simeq Q$. Thus $Z1_R \cap tR = 0$ and so R/tR is isomorphic to a subring D of Q such that $Z \subseteq D \subseteq Q$. Now suppose that m/n is in D where m and n are relatively prime. Then there are integers s and t such $sm + tn = 1$, and so $sm/n + t = (sm + tn)/n = 1/n$ is in D. Thus $R/tR \simeq Z[X_0^{-1}]$ for some set X_0 of prime numbers.

Since the first case, where $R_Q \simeq 0$, gives our result, the rest of the proof consists of a detailed analysis of the second case, where $R_Q \simeq Q$.

Consider the following diagram:

$$\begin{tikzcd}
Z \arrow[r, "f", "\text{epi}"'] & R \arrow[r] \arrow[d] & R \otimes Z[{X_0}^{-1}] \\
 & R/tR \arrow[r, "\simeq"'] & Z[{X_0}^{-1}] \arrow[u]
\end{tikzcd}$$

For n in Z, the upper route gives $n \longrightarrow n1 \longrightarrow n1 \otimes 1 = 1 \otimes n$ while the lower route gives $n \longrightarrow n1 \longrightarrow n1 + tR \longrightarrow n \longrightarrow 1 \otimes n$. Since R is an epimorph of Z, this shows that the rectangle commutes. We note that the kernel of the lower route is tR, while the kernel of the upper route is $\oplus_{p \in X_0} t_p(R)$. Thus

$$tR = \oplus_{p \in X_0} t_p(R).$$

Given an element r in tR, there exists $r_1, r_2, \ldots, r_k$ where the r_i are in $t_{p_i}(R)$ such that $r = r_1 + \cdots + r_k$. We denote by $e_{p_i} : tR \longrightarrow t_{p_i}(R)$ the map which sends r to r_i. For $\bar{r}$ in R we see that $\bar{r}r$ is in tR and $e_{p_i}(\bar{r}r) = \bar{r}r_i = \bar{r}e_{p_i}(r)$.

Let g denote the isomorphism $Z[{X_0}^{-1}] \longrightarrow R/tR$. For m/n in $Z[{X_0}^{-1}]$ we let a' be the element of R such that $g(m/n) = a' + tR$. Since $g(m) = g(m/n)g(n)$, we have $m + tR = (a' + tR)(n + tR) = na' + tR$ and so $na' - m$ is an element of tR. If b is an element of R such that $nb - m$ belongs to tR, then $n(a' - b)$ in tR gives $a' - b$ in tR, so that $a' + tR = b + tR$. So for m/n in $Z[X_0^{-1}]$, if $g(m/n) = a' + tR$ then $na' - m$ is in tR; and conversely, if b is in R such that $nb - m$ belongs to tR, then $g(m/n) = b + tR$.

Let $X_1 = \{p \in Z \mid p \text{ is prime}, t_p(R) \neq 0\}$. We note that $X_1 \subseteq X_0$, since $tR = \oplus_{p \in X_0} t_p(R)$.

Fix p in X_1 and choose a in R such that $g(1/p) = a + tR$. Therefore $1 - pa$ is in tR. Thus $(pa)^{(l-1)} - (pa)^l$ is in tR for all $l \geq 1$. For a given $l \geq 1$, the assumption that $1-(pa)^{(l-1)}$ is in tR implies that

$$(1-(pa)^{(l-1)})+((pa)^{(l-1)}-(pa)^l)=1-(pa)^l$$

belongs to tR. Thus we see that, by induction, $1-(pa)^l$ is an element of tR for all $l \geq 1$.

Since $e_p(1-pa)$ is in $t_p(R)$, we can choose a positive integer c which is minimal such that $p^c e_p(1-pa)=0$, which implies $e_p(p^c-p^c pa)=0$. Thus, $e_p(p^c(pa)^{(l-1)}-p^c(pa)^l)=0$ for all positive integers l. For each positive integer l, the assumption that $e_p(p^c-p^c(pa)^{(l-1)})=0$ implies that

$$e_p(p^c-p^c(pa)^{(l-1)})+e_p(p^c(pa)^{l-1}-p^c(pa)^l)=0,$$

so that $e_p(p^c-p^c(pa)^l)=0$. Thus we see that, by induction on l, $e_p(p^c-p^c(pa)^l)=0$ for all $l \geq 1$, so since the map e_p is additive, $p^c e_p(1-(pa)^l)=0$.

For any x in $t_p(R)$, there exists a positive integer w such that $p^w x=0$, so that $p^c(pa)^w x=0$. Now $e_p((p^c(pa)^w-p^c)x)=0$ since $p^c e_p(1-(pa)^w)=0$, but x in $t_p(R)$ implies that $(p^c(pa)^w-p^c)x$ is in $t_p(R)$. Thus

$$e_p((p^c(pa)^w-p^c)x)=(p^c(pa)^w-p^c)x,$$

so $(p^c(pa)^w-p^c)x=0$ which implies that $p^c x=0$, and so $p^c t_p(R)=0$.

Let $e(p)=e_p(1-(pa)^c)$. For any x in $t_p(R)$,

$$e(p)x=e_p((1-(pa)^c)x)=e_p(x-p^c x a^c)=e_p(x)=x.$$

Thus $e(p)$ is an identity element for $t_p(R)$, and $R=R(1-e(p))\oplus Re(p)$.

There are two cases to consider:

<u>Case I:</u> X_1 is finite. For notation, let $X_1=\{p_1,\cdots,p_k\}$. Let $e=e(p_1)+\cdots+e(p_k)$. Then e is an identity element for $\oplus_{i=1}^k t_{p_i}(R)$. Now, $R=R(1-e)\oplus Re=R(1-e)\oplus tR$ so that $R/tR\simeq R(1-e)$. Consider the maps $Z\longrightarrow R\longrightarrow$

$R/R(1-e(p)) \cong Re(p)$. Since this composition is an epimorphism, it follows from (1) at the beginning of the proof that this map is onto and so $Re(p) \cong Ze(p) \cong Z/(p^c)$. Thus

$$R \simeq R/tR \oplus Z/({p_1}^{n_1}) \oplus \cdots \oplus Z/({p_k}^{n_k}) \simeq Z[{X_0}^{-1}] \oplus Z/({p_1}^{n_1}) \oplus \cdots \oplus Z/({p_k}^{n_k})$$

as desired.

Case II: X_1 is infinite. For any p in X_1, define $S_p : R \longrightarrow t_p(R)$ by $S_p(r) = re(p)$. Define $S : R \longrightarrow \prod_{p\in X_1} t_p(R)$ by

$$S(r) = (S_{p_1}(r), S_{p_2}(r), \cdots) = (re(p_1), re(p_2), \cdots).$$

Clearly, S is a ring homomorphism.

For any r in R we choose a and b such that $r = a + b$ where there exists m/n in $Z[{X_0}^{-1}]$ with $na - m$ in tR, and b is in tR. Thus $S(r) = S(a) + S(b)$, and since b belongs to tR, there exists a positive integer k such that $S_{p_i}(b) = 0$ for all $i > k$, so that $S_{p_i}(r) = S_{p_i}(a) = e(p_i)a$. Since $na - m$ belongs to tR, there exists a positive integer $\bar{k}$ such that $e(p_i)(na - m) = 0$ for all $i > \bar{k}$, which implies that $ne(p_i)a - e(p_i)m = 0$. Hence we see that S is into the subring $\bar{R}$ of the ring $\prod_{p\in X_1} t_p(R)$, consisting of sequences of the form $\langle u_i \rangle$ where there is an element m/n in $Z[{X_0}^{-1}]$ and a positive integer l such that u_i has the form $\bar{m}/\bar{n}$ in $Ze(p_i)$ (which is isomorphic to $Z/(p_i^{n_i})$ for some n_i) for all $i > l$.

We see that S is one-to-one, for if $S(r) = 0$ then $S_{p_i}(a) = e(p_i)a = 0$ for infinitely many p_i. Therefore $m = 0 \bmod p_i^{n_i}$ for infinitely many p_i, so that $m = 0$, and so na is an element of tR. Thus r belongs to tR so $r = 0$ since $e(p_i)r = 0$ for all i.

We also see that S is onto $\bar{R}$, for let $v = (a_1, a_2, \ldots)$ be in $\bar{R}$. Since v is in $\bar{R}$, there is an element m/n in $Z[X_0^{-1}]$ such that a_i has the form $\bar{m}/\bar{n}$ in

$Z/(p_i^{n_i})$ for almost all i. Because $R/tR \simeq Z[X_0^{-1}]$ we can choose $a+tR$ in R/tR such that $na - m$ is in tR. Hence $S_{p_i}(na - m) = 0$ for almost all i, therefore $S_{p_i}(a) = a_i = \bar{m}/\bar{n}$ for almost all i. Thus there exists a positive integer l such that $S_{p_i}(a) = a_i$ for all $i > l$. Let $\bar{a} = a + \sum_{i=1}^{l}(a_i - ae(p_i))$, an element of R. Then $S(\bar{a}) = v$, and so S is onto R. Thus $R \simeq \bar{R}$, as desired, completing the proof.

∎

Thus we have proven one of the main results of this section, which gives the only possible structures of a Z-epimorph. We now show the converse, and deal with each of the three structures described in Lemma 1.2.7 separately.

Lemma 1.2.8 *For any ideal I of Z, Z/I is an epimorph of Z.*

Proof. The canonical homomorphism $f : Z \longrightarrow Z/I$ is onto. ∎

Lemma 1.2.9 *Let $R = D \oplus Z/({p_1}^{n_1}) \oplus \cdots \oplus Z/({p_k}^{n_k})$ where the p_i are primes, the n_i are positive integers, and D is a ring which is divisible by the p_i with $Z \subseteq D \subseteq Q$. Then R is an epimorph of Z.*

Proof.

Let $R = D \oplus Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$ be as in the statement of the lemma, and suppose that $g, h : R \longrightarrow S$ are ring homomorphisms such that $g(1_R) = h(1_R)$.

For each $d \in D$ let $[d]$ denote the element $(x, a_1, \cdots, a_k) \in R$ such that $x = d$, $a_1 = 0$ and $a_i = \bar{d}$ in $Z/(p_i^{n_i})$ for $1 < i \leq k$.

Since $[1/p_1^{n_1}]p_1^{2n_1}1_R = p_1^{n_1}1_R$, g and h agree on $[1/p_1^{n_1}]p_1^{2n_1}1_R$. Thus,

$$\begin{aligned} g([1]) &= g([1/p_1^{n_1}]p_1^{2n_1}1_R[1/p_1^{n_1}]) \\ &= g([1/p_1^{n_1}]p_1^{2n_1}1_R)g([1/p_1^{n_1}]) \\ &= h([1/p_1^{n_1}]p_1^{2n_1}1_R)g([1/p_1^{n_1}]) \end{aligned}$$

$$\begin{aligned}
&= h([1/p_1^{n_1}])p_1^{2n_1}1_S g([1/p_1^{n_1}]) \\
&= h([1/p_1^{n_1}])g(p_1^{2n_1}1_R[1/p_1^{n_1}]) \\
&= h([1/p_1^{n_1}])h(p_1^{2n_1}1_R[1/p_1^{n_1}]) \\
&= h([1/p_1^{n_1}]p_1^{2n_1}1_R[1/p_1^{n_1}]) \\
&= h([1]).
\end{aligned}$$

Since g and h agree on $1_R = (1, \bar{1}, \bar{1}, \cdots, \bar{1})$ and $-[1] = (-1, 0, -\bar{1}, -\bar{1}, \cdots, -\bar{1})$, they agree on their sum, that is, they agree on $(0, \bar{1}, 0, 0, \cdots, 0)$. Hence g and h agree on $Z/(p_1^{n_1})$. Using the same argument on the other coordinates, g and h agree on $Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$.

Let $1/b \in D$ for some $b \in Z$ and let $x = (1/b, \bar{1}, \bar{1}, \cdots, \bar{1})$ and $y = (b, \bar{1}, \bar{1}, \cdots, \bar{1})$. Then $xy = 1_R$ and $g(y) = h(y)$ since $y = b1_R - (0, \overline{b-1}, \overline{b-1}, \cdots, \overline{b-1})$, so $1_S = g(xy) = g(x)g(y) = g(x)h(y)$ and $1_S = h(xy) = h(yx) = h(y)h(x)$. Now $g(x) = g(x)1_S = g(x)h(y)h(x) = 1_S h(x) = h(x)$. Now since g and h agree on $Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$ it follows that $g(1/b, 0, 0, \cdots, 0) = h(1/b, 0, 0, \cdots, 0)$. Hence g and h also agree on D, so $g = h$. ■

We now consider the third structure of Lemma 1.2.7.

Lemma 1.2.10 *Let $X = \{p_1, p_2, p_3, \ldots\}$ be an infinite set of primes, $\{n_1, n_2, n_3, \ldots\}$ an infinite set of positive integers, and let D be a ring such that $Z \subseteq D \subseteq Q$ and D is divisible by each p_i in X. Let R be the subring of $\prod_{i=1}^{\infty} Z/({p_i}^{n_i})$ consisting of sequences of the form $\langle u_i \rangle$, where there is an element a/b in D such that for almost all i, u_i has the form $\bar{a}/\bar{b}$ in $Z/({p_i}^{n_i})$. Then R is an epimorph of Z.*

Proof. Fix an element p_j in X. For all $i \neq j$, let $h_{ji} : Z[1/p_j] \longrightarrow Z/({p_i}^{n_i})$ be the homomorphism where, for n in Z, $h_{ji}(n) = n + ({p_i}^{n_i})$ and $h_{ji}(1/p_j) = m + ({p_i}^{n_i})$ where m is chosen so that $1 - p_j m$ is an element of $({p_i}^{n_i})$; this is possible since p_j and p_i are relatively prime, so that we can choose integers m and $\bar{m}$ such that $mp_j + \bar{m}{p_i}^{n_i} = 1$.

In this way, we consider h_{ji} to be the "natural" homomorphism from $Z[1/p_j]$ into $Z/(p_i^{n_i})$. Let $h_{jj} : Z[1/p_j] \longrightarrow Z/(p_j^{n_j})$ be the zero map.

We now define the map $h_j : Z[1/p_j] \longrightarrow R$ by $h_j(a) = \langle h_{ji}(a) \rangle$. Since the h_{ji} maps are homomorphisms, we see that h_j preserves addition and multiplication.

Fix $a = p_{j+1}/p_j$, $b = p_{j+2}/p_j$ in $Z[1/p_j]$. Since p_{j+1} and p_{j+2} are relatively prime, we see that $(Za+Zb)(p_j) = p_{j+1}Z + p_{j+2}Z = Z$. Let $J = h_j(Za+Zb)$ and $I = p_j Z1_R$. Thus we have $JI = h_j((Za+Zb)(p_j Z)) = h_j(Z)$, and so $J^2 I = J$ and $JI^{k+1} = I^k$ for all positive integers k.

Let g_1, $g_2 : R \longrightarrow S$ be two ring homomorphisms such that $g_1(1_R) = g_2(1_R)$. Let c, d be elements of J^{n_j+1} and e be an element of I^{2n_j+1}. Then ce and ed are in $J^{n_j+1}I^{2n_j+1} = (JI)^{n_j+1}I^{n_j} \subseteq h_j(Z)(p_j Z1_R)^{n_j} = p_j^{n_j} Z1_R \subseteq Z1_R$, so $g_1(ce) = g_2(ce)$ and $g_1(ed) = g_2(ed)$. Since e is in $I^{2n_j+1} \subseteq Z1_R$, $g_1(e) = g_2(e)$ and therefore

$$\begin{aligned} g_1(ced) &= g_1(ce)g_1(d) \\ &= g_2(ce)g_1(d) \\ &= g_2(c)g_2(e)g_1(d) \\ &= g_2(c)g_1(e)g_1(d) \\ &= g_2(c)g_1(ed) \\ &= g_2(c)g_2(ed) \\ &= g_2(ced). \end{aligned}$$

Thus we see that g_1 and g_2 agree on

$$J^{n_j+1}I^{2n_j+1}J^{n_j+1} = (JI)^{2n_j+1}J = J.$$

Therefore g_1 and g_2 agree on $h_j(a)$ and $h_j(b)$. Since $a = p_{j+1}/p_j$ and $b = p_{j+2}/p_j$, there are integers α and β such that $\alpha a + \beta b = 1/p_j$. Thus g_1 and g_2 agree on $h_j(Z[1/p_j])$, for all p_j in X.

Since $(h_{n+1}(1)-h_n(1))(h_{n+2}(1)-h_n(1)) = \langle u_i \rangle$ where $u_n = 1$ and $u_m = 0$ if $m \neq n$, g_1 and g_2 agree on $\oplus_{p_i \in X} Z/(p_i^{n_i})$. Now suppose that $w/y \in D$ where $y = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Fix an integer $M > k$ and let $\langle u_i \rangle \in R$ be the element determined by $u_i = 0$ for all $i \leq M$ and $u_i = \bar{w}/\bar{y}$ for $i > M$. Then

$$\langle u_i \rangle = w h_1\left(\frac{1}{p_1^{\alpha_1}}\right) \cdots h_k\left(\frac{1}{p_k^{\alpha_k}}\right) h_{k+1}(1) \cdots h_M(1)$$

and so g_1 and g_2 agree on all elements of this form. Since every element in R is a sum of an element of this form and an element of $\oplus_{p_i \in X} Z/(p_i^{n_i})$, g_1 and g_2 agree on R, proving the lemma.

■

We now state the main result of this section, which gives all of the epimorphs of the ring of integers.

Theorem 1.2.1 *A ring R is an epimorph of Z if and only if it has one of the following forms:*

(A) R is isomorphic to Z/I for some ideal I of Z;

(B) R is isomorphic to $D \oplus Z/({p_1}^{n_1}) \oplus \cdots \oplus Z/({p_k}^{n_k})$ where the p_i are primes, the n_i are positive integers, and D is a ring such that $Z \subseteq D \subseteq Q$ and D is divisible by the p_i; or

(C) R is isomorphic to a subring of $\prod_{i=1}^{\infty} Z/(p_i^{n_i})$, for some infinite set of primes $\{p_i\}$ and positive integers n_i, consisting of all sequences of the form $\langle u_i \rangle$, where for all almost all i, $u_i = \bar{a}/\bar{b}$ in $Z/(p_i^{n_i})$ for some element a/b in a ring D, where D is such that $Z \subseteq D \subseteq Q$ and D is divisible by each prime p_i.

Hereafter, a Z-epimorph will be said to have either <u>form A</u>, <u>form B</u> or <u>form C</u> if it corresponds to (A), (B), or (C), respectively, of Theorem 1.2.1.

§1.3 The Characteristic Function

Let $h : S \longrightarrow T$ be a homomorphism of rings with identity. The maximum epimorphic extension of $h(S)$ in T will be denoted by $maxepi(h, T)$. In the special case where $S = Z$, $maxepi(h, T)$ will be denoted by $K(T)$. The following lemma shows that $maxepi(h, T)$ exists.

Lemma 1.3.1 *If $h : S \longrightarrow T$ is a homomorphism of rings with identity then there exists a maximum epimorphic extension $maxepi(h, T)$ of $h(S)$ in T.*

Proof. We see that T contains at least one epimorph of S, namely $h(S)$. Let $\{U_i\}$ be the set of all epimorphic extensions of $h(S)$ in T, and let U be the subring of T generated by the U_i. We note that $h(S)$ is a subring of U.

Suppose $g_1, g_2 : U \longrightarrow V$ are two homomorphisms of rings with identity such that $g_1 \circ h = g_2 \circ h$, so that we have the following situation:

$$S \xrightarrow{h} h(S) \subseteq U \underset{g_2}{\overset{g_1}{\rightrightarrows}} V.$$

Let x be an element of U. Then either x is an element of one of the U_i, in which case $g_1(x) = g_2(x)$ since the U_i are epimorphs of S, or x is in a subring generated by elements u_i each of which belongs to one of the U_i, in which case $g_1(x) = g_2(x)$ since g_1 and g_2 are ring homomorphisms. Thus $g_1 = g_2$ and U is the maximum epimorphic extension of $h(S)$ in T. ■

Lemma 1.3.2 *Let $\varphi : R \longrightarrow T$ be a homomorphism of rings with identity. Then $\varphi(K(R))$ is a subring of $K(T)$.*

Proof.

Since $K(T)$ is a maximal epimorphic extension, it suffices to show that $\beta : Z \rightarrow \varphi(K(R))$ is an epimorphism. Let $\gamma, \delta : \varphi(K(R)) \rightarrow V$ be two homomorphisms into the ring V such that $\gamma \circ \beta = \delta \circ \beta$. We examine the following diagram.

$$\begin{tikzcd} Z \arrow[r, "\alpha"] \arrow[rr, bend right, "\beta"'] & K(R) \arrow[r, "\varphi"] & \varphi(K(R)) \arrow[r, shift left, "\gamma"] \arrow[r, shift right, "\delta"'] & V. \end{tikzcd}$$

Since β is unique, $\beta = \varphi \circ \alpha$. Hence $\gamma \circ \varphi \circ \alpha = \delta \circ \varphi \circ \alpha$. Since α is an epimorphism $\gamma \circ \varphi = \delta \circ \varphi$ and so $\gamma = \delta$ since they agree on their common domain $\varphi(K(R))$.

■

Definition 1.3.1 For a ring A, the <u>annihilator</u> of A in Z is $ann\, A = \{z \in Z \mid zA = 0\}$.

□

We note that $ann\, A$ is an ideal of Z.

Definition 1.3.2 Let A be a ring. The <u>characteristic function</u> of A is the function $g : P \rightarrow N \cup \{\pm\infty\}$ defined as follows.

If $0 \neq ann\, A = (p_1^{n_1} \cdots p_k^{n_k})$, then $g(p_i) = n_i$ for $i = 1, \ldots, k$ and $g(q) = -\infty$ for $q \in P \setminus \{p_1, \ldots, p_k\}$.

If $ann\, A = 0$ and $p \in P$, then $g(p) = +\infty$ unless $ann\, t_p(A) = (p^k)$ for some $k \in N$ and $A = t_p(A) \oplus A^{(p)}$ where $A^{(p)}$ is an ideal of A which is p-divisible, in which case $g(p) = k$.

□

Example 1.3.1 *1. Let $A = Z/(12)$. Then $g(2) = 2$, $g(3) = 1$, and $g(p) = -\infty$ for any prime $p > 3$.*

2. Let $A = Z[1/2, 1/3, 1/5] \oplus Z/(12)$. Then $g(2) = 2$, $g(3) = 1$, $g(5) = 0$ and $g(p) = +\infty$ for all primes $p > 5$.

3. *Let $p_1, p_2, \ldots, p_i, \ldots$ be an enumeration of the primes in P, and let A be the subring of $\prod_{i=1}^{\infty} Z/(p_i^i)$ consisting of all sequences of the form $\langle u_i \rangle$ where, for almost all i, $u_i = \bar{q}$ in $Z/(p_i^i)$ for some rational number $q \in Q$. Then $g(p_i) = i$ for all primes p_i since $annt_{p_i}(A) \cong Z/(p_i^i)$ and $A = t_{p_i}(A) \oplus B$ where B is the ideal of A consisting of all $\langle u_j \rangle \in A$ such that $u_i = 0$.*

4. *We now introduce the notion of quasi-cyclic groups. Let p be a fixed prime integer, and let*

$$Z_{p^\infty} = \left\{ \frac{a}{p^n} \,\middle|\, n \in Z, n \geq 1, a \in Z, 0 \leq a < p^n \right\}.$$

Define addition $(+)$ as follows:

$$\frac{a}{p^n} + \frac{b}{p^m} = \frac{ap^m + bp^n}{p^{n+m}} (mod\, 1).$$

Then $(Z_{p^\infty}, +)$ is a quasi-cyclic group. We note that Z_{p^∞} is also called a "group of type p^∞". We view Z_{p^∞} as a ring by defining multiplication as the zero multiplication. If $A = Z_{p^\infty}$, then the characteristic function g of A is such that $g(q) = 0$ if $q \neq p$ and $g(p) = +\infty$.

Definition 1.3.3 Let A be a ring.

1. <u>$End\,A$</u> denotes the ring of endomorphisms of the right A-module, A_A.

2. <u>A^0</u> is the ring with the same underlying additive group as A and with trivial multiplication; that is, $xy = 0$ for all x, y in A^0.

□

Proposition 1.3.1 *For any ring A, $End\,A$, A^0 and A have the same characteristic function.*

Proof. Since $ann\, A = ann\, A^0 = ann\, End\, A$, if these annihilators are non-zero then the three characteristic functions coincide.

Assume that the annihilators are 0.

Suppose that $p \in P$, $ann\, t_p(A) = (p^k)$ for some $k \in N$ and $A = t_p(A) \oplus A^{(p)}$ where $A^{(p)}$ is an ideal of A which is p-divisible. Then A^0 has a corresponding direct sum decomposition, $A^0 = (t_p(A))^0 \oplus (A^{(p)})^0$ which shows that the characteristic functions of A and A^0 agree on p.

Now suppose that $p \in P$, $ann\ t_p(A^0) = (p^k)$ and $A^0 = t_p(A^0) \oplus B$ where B is an ideal of A^0 and B is p-divisible.

We first check that $t_p(EndA) = \{\theta \in End\, A \mid \theta(A) \subseteq t_p(A)\}$. We note that $t_p(A) = t_p(A^0)$. Suppose $\alpha \in t_p(End\, A)$. Then $p^m\alpha = 0$ for some $m \in N$ and so $p^m\alpha(a) = 0$ for all $a \in A$. Thus $\alpha(A) \subseteq t_p(A)$. Since the reverse inclusion is clear, $t_p(EndA) = \{\theta \in End\, A \mid \theta(A) \subseteq t_p(A)\}$ and, moreover, $p^k \in ann\ t_p(EndA)$.

Define the homomorphism $\pi : A^0 \longrightarrow t_p(A^0)$ by $\pi(a) = a'$, where $a = a' + b$ for some $a' \in t_p(A^0)$ and $b \in B$. If $p^m t_p(End\, A) = 0$, then $p^m\pi = 0$, so p^m is in (p^k). Hence $ann\ t_p(End\, A) = ann\ t_p(A^0)$.

Let $\theta \in End\, A$ and $x \in B$. Since B is p-divisible there is a $y \in B$ such that $x = p^k y$. Since $\theta(y) \in A^0$, $\theta(y) = u + v$ where $u \in t_p(A^0)$ and $v \in B$. Hence $\theta(x) = \theta(p^k y) = p^k u + p^k v = p^k v$ is in B, so $\theta(B) \subseteq B$. Let $\hat{B} = \{\alpha \in End\, A \mid \alpha(A) \subseteq B\}$. The set $\hat{B}$ is clearly a right ideal of $End\, A$ and it is a left ideal because $\theta(B) \subseteq B$ for all θ in $End\, A$.

We now show that $\hat{B}$ is p-divisible. Let α be in $\hat{B}$. For each x in A, $\alpha(x)$ is in B, so $\alpha(x) = py$ for some y in B. Moreover, y is unique because if z is in B and $py = pz$, then $p(y - z) = 0$ from which we see that $y - z$ is in $t_p(A^0) \cap B = 0$. Hence the function γ defined by $\gamma(x) = y$ is well-defined. Since α is in $End\, A$ it follows that γ is in $End\, A$, and γ is in $\hat{B}$ since $\gamma(A) \subseteq B$. Hence $\alpha = p\gamma$, so $\hat{B}$ is $p-$divisible.

Let α be in $\hat{B} \cap t_p(EndA)$. Then $\alpha = p^k\beta$ for some β in $\hat{B}$, and $p^k\alpha = 0$. Thus

$\beta \in t_p(EndA)$, so $\alpha = p^k\beta = 0$. Hence $\hat{B} \cap t_p(EndA) = 0$.

Let $\theta \in End\,A$, and let $x \in A$, $x = u + v$ where $u \in t_p(A^0)$, $v \in B$. Define θ_1 and θ_2 by $\theta_1(x) = u$ and $\theta_2(x) = v$. Clearly $\theta_1, \theta_2 \in End\,A$ and since $\theta_1(A) \subseteq t_p(A)$ and $\theta_2(A) \subseteq B$, $\theta_1 \in t_p(EndA)$ and $\theta_2 \in \hat{B}$. Because $\theta = \theta_1 + \theta_2$ this shows that $End\,A = t_p(EndA) \oplus \hat{B}$. From this we see that the characteristic functions of A^0 and $End\,A$ agree on p.

Finally, suppose that $p \in P$, $ann\,t_p(EndA) = (p^k)$ for some $k \in N$ and $End\,A = t_p(EndA) \oplus C$ where C is an ideal of $End\,A$ which is p-divisible. For each $a \in A$ define $\hat{a}$ by $\hat{a}(x) = ax$ for all $x \in A$. We see that $\hat{a} \in EndA$.

Let $M = \sum\{\theta(A) \mid \theta \in C\}$. Since each $\theta(A)$ is closed under addition, so too is M. If $\theta \in C$ and $a \in A$, then $\hat{a}\theta \in C$. Hence, for $a \in A$ and $\theta(x) \in M$, $a\theta(x) = (\hat{a}\theta)(x) \in M$. Hence M is a left ideal, and it is also a right ideal because for $a \in A$ and $\theta(x) \in M$, $\theta(x) \cdot a = \theta(xa) \in M$.

Let $m = \theta_1(a_1) + \cdots + \theta_n(a_n) \in M$, where $\theta_1, \ldots, \theta_n \in C$. Since C is p-divisible, there are $\alpha_i \in C$ such that $\theta_i = p\alpha_i$ for all $i = 1, \ldots, n$. Thus $m = p(\alpha_1(a_1) + \cdots + \alpha_n(a_n))$, so M is p-divisible.

Let i be the identity endomorphism in $End\,A = t_p(EndA) \oplus C$. Then $i = \alpha + \beta$ for some $\alpha \in t_p(EndA)$ and $\beta \in C$. Let $a \in t_p(A)$. Then $p^m a = 0$ for some $m \in N$ and $\beta = p^m\gamma$ for some $\gamma \in C$ since C is p-divisible. Now $a = i(a) = \alpha(a) + \beta(a) = \alpha(a) + p^m\gamma(a) = \alpha(a) + \gamma(p^m a) = \alpha(a) + \gamma(0) = \alpha(a)$. Hence $t_p(A) \subseteq \alpha(A)$, and since $\alpha \in t_p(EndA)$, $\alpha(A) \subseteq t_p(A)$. Thus $t_p(A) = \alpha(A)$, and $p^k \in ann\,t_p(A)$. Suppose $\ell \in ann\,t_p(A)$. Then $\ell\alpha = 0$ because $t_p(A) = \alpha(A)$. Also, since $i = \alpha + \beta$, $t_p(EndA) = \alpha End\,A$ and so $\ell \in ann\,t_p(End\,A) = (p^k)$. Thus $ann\,t_p(A) = ann\,t_p(End\,A)$.

Since $ann\ t_p(A) = (p^k)$ and M is p-divisible, it follows that $t_p(A) \cap M = 0$. Also, if $a \in A$, $a = i(a) = \alpha(a) + \beta(a) \in t_p(A) + M$, so $A = t_p(A) \oplus M$. From this we see that the characteristic functions of $End\,A$ and A agree on p.

Therefore, we see that A, A^0 and $End\,A$ have the same characteristic function. ■

Proposition 1.3.2 *If A and B are rings with the same characteristic function g, then g is the characteristic function of $A \oplus B$.*

Proof. If $p \in P$ and $A = t_p(A) \oplus A^{(p)}$ where $ann\,t_p(A) = (p^k)$ for some $k \in N$ and $A^{(p)}$ is an ideal of A which is p-divisible, then B has a similar decomposition $B = t_p(B) \oplus B^{(p)}$ which gives rise to the decomposition $A \oplus B = (t_p(A) \oplus t_p(B)) \oplus (A^{(p)} \oplus B^{(p)})$.

Conversely, if $A \oplus B = t_p(A \oplus B) \oplus C$ where $ann\,t_p(A \oplus B) = (p^k)$, $k \in N$ and C is an ideal of $A \oplus B$ which is p-divisible, then we obtain direct sum decompositions $A = t_p(A) \oplus X_A$, $B = t_p(B) \oplus X_B$ as follows. Let $X_A = C \cap A$. Then X_A is an ideal of A and, since $t_p(A) \subseteq t_p(A \oplus B)$, $t_p(A) \cap X_A = 0$.

Let $\alpha \in A$, $\beta \in B$ and suppose $\alpha + \beta \in C$. Then $\alpha = u + v$ where $u \in t_p(A \oplus B)$ and $v \in C$. Thus $p^k\alpha = p^k v \in C$ and so $p^k\alpha = p^{k+1}\gamma$ for some $\gamma \in C$. Since $C \cap t_p(A \oplus B) = 0$, $\alpha = p\gamma$ so $\alpha \in C$.

Let $a \in A$. Then $a = (a_1 + b_1) + (\alpha + \beta)$ where $a_1 + b_1 \in t_p(A \oplus B)$, $\alpha + \beta \in C$, $a_1, \alpha \in A$ and $b_1, \beta \in B$. Since the sum $A + B$ is direct, $a = a_1 + \alpha$ and from above $\alpha \in A \cap C$. Hence $A = t_p(A) \oplus (C \cap A)$.

If $a \in C \cap A$, $a = pc$ for some $c \in C$. Now $c = a_1 + b_1$, $a_1 \in A$, $b_1 \in B$ and so $a = pc = pa_1 + pb_1$. Since $A + B$ is direct, $a = pa_1$ and from above $a_1 \in C$. Hence $C \cap A$ is p-divisible. Similarly, $B = t_p(B) \oplus (C \cap B)$. Since A and B have the same characteristic function, $ann\,t_p(A) = ann\,t_p(B)$ and since $t_p(A \oplus B) = t_p(A) \oplus t_p(B)$, $ann\,t_p(A \oplus B) = ann\,t_p(A) = ann\,t_p(B)$.

It follows that $A \oplus B$ has characteristic function g. ■

Lemma 1.3.3 *Let $\varphi : S \to T$ be a homomorphism of rings with identity and let g_S, g_T be the characteristic functions of S and T, respectively. Then $g_T(p) \leq g_S(p)$ for all p in P.*

Proof. Since $\varphi(S)$ is a unital subring of T, $ann\,T = ann\,\varphi(S) \supseteq ann\,S$. Thus if $ann\,T \neq 0$ it is clear that $g_T(p) \leq g_S(p)$ for all $p \in P$.

Now assume $ann\,T = 0$. Since $ann\,T \supseteq ann\,S$ this implies that $ann\,S = 0$. If $g_S(p) = 0$, then $t_p(S) = \{0\}$ and S is p-divisible. Hence $\varphi(S)$ is p-divisible and so T is also p-divisible because $\varphi(S)$ and T have the same identity. Suppose $x \in T$ is such that $p^m x = 0$. Let $1 = p^m v$ for some $v \in T$. Then $x = 1 \cdot x = p^m v x = 0$, so $t_p(T) = 0$. Hence $g_T(p) = 0$.

Now suppose that $0 < g_S(p) = k < \infty$. Then $S = t_p(S) \oplus S^{(p)}$ where $S^{(p)}$ is an ideal of S which is p-divisible and $ann\,t_p(S) = (p^k)$. Let $1_S = e + f$ where $e \in t_p(S)$ and $f \in S^{(p)}$. Then $1_{\varphi(S)} = 1_T = \varphi(e) + \varphi(f)$. Let $x_1 \in t_p(T)$. Then $p^m x_1 = 0$ for some integer m. Since $S^{(p)}$ is p-divisible, $f = p^m s$ for some $s \in S$ and hence $x_1 = 1 \cdot x_1 = \varphi(e)x_1 + \varphi(f)x_1 = \varphi(e)x_1 + \varphi(s)p^m x_1 = \varphi(e)x_1 \in \varphi(e)T$. So $t_p(T) = \varphi(e)T$. Similarly, $t_p(T) = T\varphi(e)$.

Let $x_2 \in T$. Since $1_T = \varphi(e) + \varphi(f)$ and $\varphi(e)\varphi(f) = \varphi(ef) = \varphi(0) = 0$,

$$\begin{aligned} x_2\varphi(f) &= (\varphi(e) + \varphi(f))x_2\varphi(f) \\ &= \varphi(e)x_2\varphi(f) + \varphi(f)x_2\varphi(f) \\ &= x_3\varphi(e)\varphi(f) + \varphi(f)x_2\varphi(f) \\ &= \varphi(f)x_2\varphi(f) \in \varphi(f)T, \end{aligned}$$

where $\varphi(e)x_2 = x_3\varphi(e)$ for some $x_3 \in T$ because $\varphi(e)T = T\varphi(e)$. It follows that $\varphi(f)T$ is an ideal of T, and $\varphi(f)T$ is p-divisible because there is an $s_1 \in S$ such that $f = ps_1 = pfs_1$ so that, for $t \in T$, $\varphi(f)t = \varphi(pfs_1)t = p\varphi(f)\varphi(s_1)t \in p\varphi(f)T$. Also, since $1_T = \varphi(e) + \varphi(f)$, $\varphi(e)T + \varphi(f)T = T$. Moreover, $\varphi(e)T \cap \varphi(f)T = 0$ because

$\varphi(e)\varphi(f) = 0$. Since $p^k e = 0$, $p^k\varphi(e)T = 0$ and so the direct sum decomposition $T = \varphi(e)T \oplus \varphi(f)T$ shows that $g_T(p) \leq k$.

Of course, if $g_S(p) = \infty$ we must have $g_T(p) \leq g_S(p)$, so the proof is complete. ■

Note that if A is a ring with characteristic function g, then g determines an epimorph E_g of the integers as follows.

If $g(p) = -\infty$ for some p, $E_g = Z/ann\, A$.

Otherwise, let $X_1 = \{p \in P \mid 0 < g(p) < \infty\}$ and $X_0 = X_1 \cup \{p \in P \mid g(p) = 0\}$. If $X_1 = \{p_1, \ldots, p_n\}$ is finite, $E_g = D \times Z/(p_1^{g(p_1)}) \times \cdots \times Z/(p_n^{g(p_n)})$ where $D = Z[1/p \mid p \in X_0]$ while if X_1 is infinite, E_g is the set of all sequences $\langle u_i \rangle$ in $\prod_{p \in X_1} Z/(p^{g(p)})$ which are eventually of the form $\bar{a}/\bar{b}$ where $a/b \in D = Z\{1/p \mid p \in X_0\}$.

Proposition 1.3.3 *If R is an epimorph of Z with characteristic function g, then $R \cong E_g$.*

Proof. If $ann\, R \neq 0$, $g(p) = -\infty$ for some p and $E_g = Z/ann\, R$. From Theorem 1.2.1, $R \cong Z/I$ for some I and this implies that $I = ann\, R$. Hence $R \cong Z/I = E_g$.

We now assume that $ann\, R = 0$. First suppose that $R \cong D \oplus Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$ where, for each i, p_i is in P, n_i is a positive integer, and D is a ring with $Z \subseteq D \subseteq Q$ which is divisible by p_i for all $i = 1, \ldots, k$. From the definition of the characteristic function it is clear that $g(p_i) = n_i$ for all $i = 1, \ldots, k$, that $g(q) = 0$ if D is q-divisible and $q \notin \{p_1, \ldots, p_k\}$, and $g(p) = \infty$ for all other primes p. Hence $E_g = D \oplus Z/(p_1^{n_1}) \oplus \cdots \oplus Z/(p_k^{n_k})$.

Now suppose that there is an infinite set of primes $\{p_1, p_2, \ldots\}$, a corresponding set of positive integers $\{n_1, n_2, \ldots\}$ and a ring D, $Z \subseteq D \subseteq Q$, divisible by all of the primes $p_1, p_2, \ldots$ such that R is isomorphic to the set of all sequences $\langle u_i \rangle$ in $\prod_{i=1}^{\infty} Z/(p_i^{n_i})$ for which there is some $a/b \in D$ such that $u_i = \bar{a}/\bar{b}$ for almost all i. For each $p_i \in \{p_1, p_2, \ldots\}$, $t_{p_i}(R) = \{\langle u_i \rangle \in R \mid u_j = 0 \text{ if } j \neq i\}$ and $R^{(p_i)} = \{\langle u_j \rangle \in R \mid u_i = 0\}$ is p_i-divisible. Thus $g(p_i) = n_i$ for all i. If $q \in P \setminus \{p_1, p_2 \ldots\}$, then $t_q(R) = 0$, so $g(q) = 0$ if D, and hence R, is q-divisible, and $g(q) = \infty$ otherwise. Hence E_g is isomorphic to R. ∎

Proposition 1.3.4 *If R is a ring with identity, then $K(R)$ and R have the same characteristic function.*

Proof. Let g_K and g denote the characteristic functions of $K(R)$ and R respectively. Since $ann\, K(R) = ann\, R$, we may assume $ann\, K(R) = ann\, R = \{0\}$. From Lemma 1.3.3, $g(p) \leq g_K(p)$ for all primes p, so we need only show that, for all $p \in P$, $g_K(p) \leq g(p)$.

Suppose $g(p) = k \in N$. Then $R = t_p(R) \oplus R^{(p)}$ where $R^{(p)}$ is an ideal of R which is p-divisible and $ann\, t_p(R) = (p^k)$. Write $1_R = e + d$ where $e \in t_p(R)$ and $d \in R^{(p)}$. Note that if $m \in Z$ and $md = 0$, then $p^k m 1_R = 0$ and so $p^k m \in ann\, R = \{0\}$, and thus $m = 0$. Since $R^{(p)}$ is p-divisible, $d = pr$ for some $r \in R^{(p)}$.

Define $\theta : Z[1/p] \to Zr$ by $\theta(f(1/p)) = f(r)$ for each $f \in Z[x]$. Suppose $f, g \in Z[x]$ and $f(1/p) = g(1/p)$. Then $(f-g)(1/p) = 0$, so $(f-g)(x) = (x - 1/p)h(x)$ for some $h(x) \in Q[x]$ and it is easy to see that in fact $h(x) \in Z[x]$. Multiplying by p and substituting r for x we obtain $p(f-g)(r) = (pr-1)h(r)$, and since $pr - 1 = d - 1 = e$ it follows that $(f-g)(r) \in t_p(R) \cap R^{(p)} = \{0\}$. Hence $f(r) = g(r)$ and so θ is well-defined.

Clearly θ is an onto homomorphism. Suppose $\theta(f(1/p)) = 0$ where $f(x) = a_0 + a_1 x + \cdots + a_m x^m$. Then $a_0 + a_1 r + \cdots + a_m r^m = 0$, and so $a_0 p^m d + a_1 p^{m-1} d + \cdots + a_{m-1} p d + a_m d = 0$. Hence $(a_0 p^m + a_1 p^{m-1} + \cdots + a_{m-1} p + a_m) d = 0$ and so $a_0 p^m + a_1 p^{m-1} + \cdots + a_{m-1} p + a_m = 0$ since we know that $md = 0$ implies $m = 0$. But this implies that $a_0 + a_1(1/p) + \cdots + a_{m-1}(1/p^{m-1}) + a_m(1/p^m) = 0$, so $f(1/p) = 0$. Hence θ is one to one.

The sum $Ze + Zr$ is direct since $Ze \subseteq t_p(R)$ and $Zr \subseteq R^{(p)}$. Since $1_R = e + pr \in Ze \oplus Zr$, and $Ze \oplus Zr$ is an epimorph of Z of form B, $Ze \oplus Zr \subseteq K(R)$ since $K(R)$

is the maximal epimorphic extension of $Z1_R$ in R.

Now, $K(R)e$ and $K(R)d$ are ideals of $K(R)$ since e and d are central idempotents. Since $1_R = e + d$, $K(R) = K(R)e + K(R)d$ and, as above, the sum is direct. Then $r = ae + bd$, for some a, $b \in K(R)$, so $ae \in Re \cap Rd = \{0\}$ and hence $r \in K(R)d$. Since $d = pr$, this shows that $K(R)d$ is p-divisible and hence $t_p(K(R)d) = \{0\}$. Since $p^k e = 0$, $p^k K(R)e = \{0\}$ and so $t_p(K(R)) = K(R)e$ and $ann\,(t_p(K(R)) = (p^\ell)$ where $\ell \leq k$. Hence $g_K(p) \leq g(p)$, as required. ■

Theorem 1.3.1 *If R is a ring with identity with characteristic function g, then $K(R) \cong E_g$.*

Proof. By the Proposition 1.3.4, $K(R)$ has characteristic function g and so $K(R) \cong Eg$ by Proposition 1.3.3. ■

We close this section with the following result which will be useful in what follows.

Proposition 1.3.5 *Let $S \subseteq T$ be rings with the same identity and characteristic functions g_S and g_T, respectively. If $g_S(p) \leq g_T(p)$ for all p, then $K(S) = K(T)$.*

Proof. We first show that one-to-one identity preserving endomorphisms of epimorphs of Z must be onto. Suppose X is a set of prime numbers, $D = Z[1/p \,|\, p \in X]$ and $\alpha : D \to D$ is a one-to-one homomorphism. Then for each $p \in X$, $\alpha(1/p) \neq 0$ and $p \cdot \alpha(1/p) = 1$. Hence $\alpha(1/p) = 1/p$. Thus α is onto.

Now let R be an arbitrary epimorph of Z and suppose that $\theta : R \to R$ is a one-to-one homomorphism. Then, for each prime p, $\theta(t_p(R)) \subseteq t_p(R)$ and since $t_p(R)$ is finite, $\theta(t_p(R)) = t_pR$. Hence $\theta(tR) = tR$ and so θ induces a one-to-one homomorphism $\hat{\theta} : R/tR \to R/tR$. Since $R/tR = Z[1/p \,|\, p \in X]$ for some set of primes X, the remarks in the above paragraph show that $\hat{\theta}$, and hence θ, is onto.

Now suppose $S \subseteq T$ are rings with the same identity and that $g_S(p) \leq g_T(p)$ for all primes p. From Lemma 1.3.3, $g_S = g_T$. We will denote this function by g. Hence from Theorem 1.3.1 $K(T) \cong Eg \cong K(S)$. Suppose $\gamma : K(T) \to K(S)$ is an isomorphism. From Lemma 1.3.2 $K(S) \subseteq K(T)$, and we denote the inclusion by $i : K(S) \longrightarrow K(T)$. The composition $i\gamma : K(T) \longrightarrow K(T)$ is a one-one-one homomorphism, and so by the first part of the proof $i\gamma$ is onto. Hence i is onto and thus $K(S) = K(T)$. ■

CHAPTER 2

Survey of Extensions

§2.1 Introduction

In this chapter we will consider various methods which have been developed which extend an arbitrary ring to a ring with identity. The first method which we will consider, which was developed by Dorroh, extends any ring R to $R \times Z$ which contains an identity element $(0, 1)$. While this construction provides an extension for any ring R, many properties of R are lost in the extension. The Dorroh extension may be generalized as $R \times Y$, where Y is a ring with identity and R is a Y-bimodule algebra.

The approach developed by Robson adjoins to a given ring R a subring of the center of *End* R, the ring of endomorphisms of R. Unlike the extension developed by Dorroh, however, this approach requires R to be left faithful. Burgess and Stewart developed a refinement to the Robson approach which uses the characteristic ring of *End* R. This refinement preserves in the extension many properties of the original ring R.

We will also investigate the special case of regular rings, and examine two approaches developed to extend a regular ring R to a regular ring with identity.

This chapter will present the various extensions, while later chapters will examine properties preserved by the extension if possessed by the original ring. Throughout this chapter, R will denote the given (arbitrary) ring.

§2.2 The Dorroh Construction

Suppose Y is a ring with identity such that R is a Y-bimodule algebra. Dorroh has demonstrated that R can be embedded in a ring S with identity, where $S = R \times Y$, and with addition and multiplication defined as follows:

$$\begin{aligned}(r_1, n_1) + (r_2, n_2) &= (r_1 + r_2, n_1 + n_2)\\(r_1, n_1)(r_2, n_2) &= (r_1r_2 + n_1r_2 + n_2r_1, n_1n_2)\end{aligned}$$

for all r_1, r_2 in R and n_1, n_2 in Y.

It is an easy exercise to show that S is a ring. The identity of S is $(0, 1)$ since

$$(r, n)(0, 1) = (r0 + n0 + 1r, n1) = (r, n) \quad \text{and}$$

$$(0, 1)(r, n) = (0r + n0 + 1r, 1n) = (r, n)$$

for all r in R and n in Y.

To see that R is embedded in S, we now show that there is an ideal of S which is isomorphic to R. Let $T = \{(r, 0) \mid r \in R\}$, an ideal of S.

Lemma 2.2.1 *R is isomorphic to T.*

Proof. Define a function $f : T \longrightarrow R$ by $f(r, 0) = r$. We note that f is a homomorphism since

$$f((r_1, 0) + (r_2, 0)) = f(r_1 + r_2, 0) = r_1 + r_2 = f(r_1, 0) + f(r_2, 0)$$

and

$$f((r_1, 0)(r_2, 0)) = f(r_1r_2, 0) = r_1r_2 = f(r_1, 0)f(r_2, 0)$$

for all r_1, r_2 in R. Further, f is one-to-one since $f(r_1, 0) = f(r_2, 0)$ implies $r_1 = r_2$, and f is onto since, for all r in R, $(r, 0)$ is in T. Therefore R is isomorphic to T, and we consider R to be embedded as an ideal of S in this way. ∎

Although R may be extended to a ring with identity $R \times Y$ using this approach, many properties possessed by the original ring R are not possessed by the extension $R \times Y$. For example, if R contains an identity 1_R, the canonical homomorphism

$f : R \longrightarrow R\times Y$ does not preserve the identity, i.e. $f(1_R) = (1_R, 0) \neq (0, 1_Y)$ which is the identity of $R \times Y$. Further, if Y does not have finite characteristic, the extension $R\times Y$ does not have finite characteristic, regardless of the characteristic of the original ring R.

In view of Corollary 1.2.1, we see that any ring R may be extended to a ring with identity, $R \times Z$, using this method.

§2.3 Complete Set of Extensions – The Brown and McCoy Construction

Brown and McCoy developed a modification of the Dorroh extension which is "minimal", by providing a set $\mathcal{S}$ of extensions of R with the following properties:

1. each S in $\mathcal{S}$ has an identity and is equipped with a monomorphism $\theta_S : R \longrightarrow S$; and
2. if T is a ring with identity and $f : R \longrightarrow T$ is a monomorphism, then T contains a subring T' such that $f(R) \subseteq T'$ and for some ring S in $\mathcal{S}$ there is an isomorphism $g : S \longrightarrow T'$ such that $g(1_S) = 1_T$ and the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, "\theta_S"] \arrow[dr, "f"'] & S \arrow[d, "g"] \\ & T' \end{tikzcd}$$

Definition 2.3.1 Such a set $\mathcal{S}$ is called a <u>complete set of extensions</u> of R. □

Definition 2.3.2 Let I be an ideal of a ring R and let μ be an integer. An element x in R is a μ-fier modulo I if $xr + I = \mu r + I$ and $rx + I = \mu r + I$ for every r in R. A μ-fier modulo(0) is called a μ-fier. □

Let $(-a, \alpha) \in R \times Z$, the Dorroh extension of R obtained by adjoining the ring of integers, where $a \in R$ and $\alpha \in Z$ are such that a is an α-fier and $a = 0$ if $\alpha = 0$. We note that $Z(-a, \alpha)$ is an ideal of $R \times Z$ since

$$(-\beta a, \beta\alpha)(r, \mu) = (-\beta ar + \beta\alpha r - \mu\beta a, \mu\beta\alpha) = (-\mu\beta a, \mu\beta\alpha)$$

and

$$(r, \mu)(-\beta a, \beta\alpha) = (-\beta ra + \beta\alpha r - \mu\beta a, \mu\beta\alpha) = (-\mu\beta a, \mu\beta\alpha)$$

for all $(-\beta a, \beta\alpha)$ in $Z(-a, \alpha)$ and all (r, μ) in $R \times Z$. The factor ring $(R \times Z)/Z(-a, \alpha)$ will be denoted by $R(a, \alpha)$, and cosets of elements (r, μ) of $R \times Z$ by $[r, \mu]$. We note that, in $R(a, \alpha)$, $[r_0, \mu_0] = [r_1, \mu_1]$ if and only if $r_1 - r_0 = -\lambda a$ and $\mu_1 - \mu_0 = \lambda\alpha$ for some λ in Z since $[r_0, \mu_0] = \{(r, \mu) \mid (r - r_0, \mu - \mu_0) = \lambda(-a, \alpha) \text{ for some } \lambda \in Z\}$.

Theorem 2.3.1 *Let $\mathcal{C} = \{R(m, \mu) \mid \mu \in Z$ and m is a μ-fier of $R\}$ and for each $S = R(m, \mu) \in \mathcal{C}$ let $\theta_S : R \longrightarrow S$ be defined by $\theta_S(r) = [r, 0]$. Then $\mathcal{C}$ is a complete set of extensions of R.*

Proof. Let T be a ring with identity and $f : R \longrightarrow T$ a monomorphism. Choose $\sigma \in N$ such that $(\sigma) = \{n \in Z \mid n1_T \in f(R)\}$. Let $m \in R$ be such that $f(m) = \sigma 1_T$. Then, for any $r \in R$, $f(mr - \sigma r) = \sigma 1_T f(r) - \sigma f(r) = 0$ and so, since f is one-to-one, $mr = \sigma r$. Hence m is a σ-fier of R and so $R(m, \sigma) \in \mathcal{C}$. Let $T' = \{f(r) + n1_T \mid r \in R, n \in Z\}$ and define $g : R(m, \sigma) \longrightarrow T'$ by $g([r, n]) = f(r) + n1_T$.

We first check that g is well-defined. If $[r_0, n_0] = [r_1, n_1]$, then $r_0 - r_1 = -km$ and $n_0 - n_1 = k\sigma$ for some $k \in Z$. Hence $f(r_0) - f(r_1) = f(r_0 - r_1) = -kf(m) = -k\sigma 1_T$ and so

$$f(r_0) + n1_T = (f(r_1) - k\sigma 1_T) + n_0 1_T = f(r_1) + (n_0 - k\sigma)1_T = f(r_1) + n_1 1_T.$$

Hence g is well-defined.

The map g is a homomorphism since

$$\begin{aligned} g([r_0,n_0]+[r_1,n_1]) &= g([r_0+r_1,n_0+n_1]) \\ &= f(r_0+r_1)+(n_0+n_1)1_T \\ &= (f(r_0)+n_01_T)+(f(r_1)+n_11_T) \\ &= g([r_0,n_0])+g([r_1,n_1]) \end{aligned}$$

and

$$\begin{aligned} g([r_0,n_0][r_1,n_1]) &= g([r_0r_1+n_1r_0+n_0r_1,n_0n_1]) \\ &= f(r_0r_1+n_1r_0+n_0r_1)+n_0n_11_T \\ &= f(r_0)f(r_1)+n_11_Tf(r_0)+n_01_Tf(r_1) \\ &+ (n_01_T)(n_11_T) \\ &= (f(r_0)+n_01_T)(f(r_1)+n_11_T) \\ &= f([r_0,n_0])f([r_1,n_1]). \end{aligned}$$

Clearly g is surjective and g is also one-to-one. To see this suppose that $g([r,n]) = 0$. Then $f(r)+n1_T = 0$ and so $n1_T = f(-r) \in f(R)$. Hence $n \in (\sigma)$, so $n = k\sigma$ for some $k \in Z$. Also $f(r) = -n1_T = -k\sigma 1_T = -kf(m) = f(-km)$ and so, since f is one-to-one, $r = -km$. Since $r = -km$ and $n = k\sigma$ we see that $[r,n] = [0,0]$. Hence g is one-to-one.

Of course $g([0,1]) = 1_T$, so it only remains to see that, with $S = R(m,\sigma)$, $g \circ \theta_S = f$. If $r \in R$, then $g \circ \theta_S(r) = g([r,0]) = f(r)$ and this completes the proof. ∎

We will now characterize those rings which have a complete set of extensions which contain only one element. In order to do this we will require the following lemma.

Lemma 2.3.1 *$Z/(\alpha)$ is a homomorphic image of $R(a,\alpha)$, where the kernel of the homomorphism is $\{[r,0] \mid r \in R\} \simeq R$.*

Proof. Define the map $h : R(a,\alpha) \longrightarrow Z/(\alpha)$ by $h([r,\mu]) = \bar{\mu}$, where $\imath$ is an α-fier and $\bar{\mu} = \mu + (\alpha)$ is in $Z/(\alpha)$. Since $[r_0,\mu_0] = [r_1,\mu_1]$ if and only if μ_1 - $\mu_0 = \lambda\alpha$ for some $\lambda \in Z$, we see that h is well defined. Thus h is a homomorphism ince

$$\begin{aligned} h([r_0,\mu_0] + [r_1,\mu_1]) &= h([r_0 + r_1, \mu_0 + \mu_1]) \\ &= \overline{\mu_0 + \mu_1} \\ &= \overline{\mu_0} + \overline{\mu_1} \\ &= h([r_0,\mu_0]) + h([r_1,\mu_1]) \end{aligned}$$

and

$$\begin{aligned} h([r_0,\mu_0][r_1,\mu_1]) &= h([r_0 r_1 + \mu_0 r_1 + \mu_1 r_0, \mu_0\mu_1]) \\ &= \overline{\mu_0\mu_1} \\ &= \overline{\mu_0}\,\overline{\mu_1} \\ &= h([r_0,\mu_0])h([r_1,\mu_1]). \end{aligned}$$

Thus $Z/(\alpha)$ is a homomorphic image of $R(a,\alpha)$. The kernel of h is

$$\begin{aligned} ker\, h &= \{[r,\mu] \mid r \in R,\ \bar{\mu} = 0\} \\ &= \{[r,\mu] \mid r \in R, \mu = \lambda\alpha \text{ for some } \lambda \in Z\} \\ &= \{[r,0] \mid r \in R\} \\ &\simeq R. \end{aligned}$$

■

Theorem 2.3.2 *A ring R has a one-element complete set of extension if and only if R has an identity or R has no μ-fiers with $\mu \neq 0$.*

Proof. Suppose that $\{S\}$ is a complete set of extensions of R with monomorphism $\theta_S : R \longrightarrow S$.

Let $\sigma > 0$ be a generator for the principal ideal $\{n \in Z \mid n \cdot 1_S \in \theta_S(R)\}$. If $\sigma = 1$, then $\theta_S(R)$, and hence R, has an identity.

We now assume that $\sigma > 1$. Let $m \in R$ be the element where $\theta_S(m) = \sigma 1_s$. Since θ_S is a monomorphism, m is unique. From the proof of Theorem 2.3.1 we see that $\psi : R(m, \sigma) \longrightarrow S$ defined by $\psi[r, n] = \theta_S(r) + n1_S$ is a monomorphism.

Let $f : R \longrightarrow R \times Z$ be defined by $f(r) = (r, 0)$. Since S is a complete set of extensions of R there is a subring T' of $R \times Z$ such that $f(R) \subseteq T'$, and an isomorphism $g : S \longrightarrow T'$ such that $g(1_S) = (0,1)$ and $g \circ \theta_S = f$. Thus we have the following sequence of homomorphisms,

$$R(m, \sigma) \xrightarrow{\psi} S \xrightarrow{g} T' \subseteq R \times Z \xrightarrow{\pi} Z$$

where $\pi(r, n) = n$ for all $(r, n) \in R \times Z$. Denote the composition of these homomorphisms by Γ. If $[r, n] \in R(m, \sigma)$, then

$$\begin{aligned} \Gamma([r, n]) &= \pi g \psi([r, n]) \\ &= \pi g(\theta_S(r) + n1_S) \\ &= \pi(g\theta_S(r) + g(n1_S)) \\ &= \pi(f(r) + (0, n)) \\ &= \pi((r, 0) + (0, n)) \\ &= \pi((r, n)) \\ &= n \end{aligned}$$

so we see that Γ is surjective and $ker\, \Gamma = \{[r, 0] \mid r \in R\}$. Hence

$$\frac{R(m, \sigma)}{\{[r, 0] \mid r \in R\}} \cong Z.$$

This contradicts Lemma 2.3.1 unless $\sigma = 0$.

Conversely, suppose that R has an identity or that R has no μ-fier, $\mu \neq 0$. If R has an identity, $\{R\}$ is a complete set of extensions.

Now suppose that R has no μ-fiers, $\mu \neq 0$. We will show that the set consisting of the Dorroh extension, $\{R \times Z\}$, is a complete set of extensions where $\iota_{R\times Z} : R \longrightarrow R \times Z$ is the usual embedding $r \longrightarrow (r, 0)$. Suppose that T is a ring with identity and $f : R \longrightarrow T$ is a monomorphism. Define $g : R \times Z \longrightarrow T$ by $g((r, n)) = f(r) + n1_T$. Then g is a homomorphism and the universal property of $R \times Z$, which we will establish in Section 3.1, tells us that the following diagram commutes. Hence it suffices to show that g is one-to-one.

$$\begin{tikzcd}
R \arrow[r, "\theta_{R\times Z}"] \arrow[dr, "f"'] & R \times Z \arrow[d, "g"] \\
& g(R \times Z)
\end{tikzcd}$$

Suppose $g((r, n)) = 0$. Then $f(r) = -n1_T$. Let $a \in R$. Then $f(ar) = f(a)f(r) = f(a)(-n1_T) = f(-na)$ and since f is a monomorphism, $ar = -na$ for all $a \in R$. Hence r is a $-n$-fier and hence $n = 0$. Since $f(r) = -n1_T = 0$ and f is one-to-one $r = 0$ also. Hence g is one-to-one. ∎

§2.4 Robson's Construction

Robson developed a construction which extends R to a ring with unity by adjoining a subring of the center of *End R*, the endomorphism ring of R. This construction requires R to be left faithful so that R embeds in *End R* by the function $g : R \longrightarrow$ *End R* where, for any r in R, $g(r)(x) = rx$ for all x in R.

We begin with the following definitions.

Definition 2.4.1 A ring R is <u>left faithful</u> if, for all r in R, $r = 0$ if $rR = 0$. □

Definition 2.4.2 The <u>center</u> of a ring S is the subring $Z(S) = \{s \in S \mid sx = xs$ for all $x \in S\}$. □

Lemma 2.4.1 *If R is left faithful then $g : R \longrightarrow End\ R$ is a monomorphism.*

Proof. Let r_1, r_2 be in R. Then

$$\begin{aligned} g(r_1 + r_2)(x) &= (r_1 + r_2)x \\ &= r_1x + r_2x \\ &= g(r_1)x + g(r_2)x \end{aligned}$$

and

$$\begin{aligned} g(r_1r_2)(x) &= (r_1r_2)x \\ &= r_1(r_2x) \\ &= (g(r_1) \circ g(r_2))(x) \end{aligned}$$

for all x in R, so g is a homomorphism.

Let y be in ker g. Then $yr = 0$ for all r in R, so $y = 0$. Thus g is one-to-one and a monomorphism. ■

The remainder of this section assumes that R is left-faithful. For each $r \in R$ we will denote $g(r)$ by $\hat{r}$ and we will denote $g(R)$ by $\hat{R}$, a subring of $End\ R$.

Lemma 2.4.2 *Let φ be in $End\ R$ and x in R. Then $\varphi\hat{x} = \widehat{\varphi(x)}$ is in $\hat{R}$.*

Proof. For all r in R,

$$\begin{aligned} (\varphi\hat{x})(r) &= \varphi(\hat{x}(r)) \\ &= \varphi(xr) \\ &= \varphi(x)r \\ &= \widehat{\varphi(x)}(r) \end{aligned}$$

so $\varphi\hat{x} = \widehat{\varphi(x)}$ is in $\hat{R}$. ■

Let C be a subring of $Z(End\ R)$ containing the identity map. Then we have the following results.

Lemma 2.4.3 *$\hat{R} + C$ is a subring of $End\ R$.*

Proof. Let $\hat{r_1}$, $\hat{r_2}$ be in $\hat{R}$ and c_1, c_2 be in C, so that $\hat{r_1} + c_1, \hat{r_2} + c_2$ are in $\hat{R} + C$. Then $(\hat{r_1} + c_1) - (\hat{r_2} + c_2) = (\hat{r_1} - \hat{r_2}) + (c_1 - c_2) = \widehat{r_1 - r_2} + (c_1 - c_2) \in \hat{R} + C$. Also, $(\hat{r_1} + c_1)(\hat{r_2} + c_2) = \widehat{r_1 r_2} + \hat{r_1}c_2 + c_1\hat{r_2} + c_1c_2 = \widehat{r_1 r_2} + c_2\hat{r_1} + c_1\hat{r_2} + c_1c_2 = \widehat{r_1 r_2} + c_2\widehat{(r_1)} + c_1\widehat{(r_2)} + c_1c_2 = \widehat{(r_1r_2 + c_2(r_1) + c_1(r_2))} + c_1c_2 \in \hat{R} + C$. ■

Definition 2.4.3 A non-zero right ideal I of a ring R is <u>essential</u> as a right ideal of R if $I \cap J \neq 0$ for all non-zero right ideals J of R. □

Lemma 2.4.4 *$\hat{R}$ is an ideal of $\hat{R} + C$, essential as a right ideal.*

Proof. Since $C \subseteq Z(End\, R)$, it follows from Lemma 2.4.2 that $\hat{R}$ is an ideal of $\hat{R} + C$. Let I be a non-zero right ideal of $\hat{R} + C$, and let $0 \neq \varphi \in I$. Then $\varphi(r) \neq 0$ for some r in R and $\varphi\hat{r} = \widehat{\varphi(r)}$ by Lemma 2.4.2. Also, by Lemma 2.4.1, $\widehat{\varphi(r)} \neq 0$ and so $I\hat{R} \neq 0$. Since $I\hat{R} \subseteq I \cap \hat{R}$, $\hat{R}$ is essential as a right ideal. ■

This approach to extend R to a ring with identity requires that R be left faithful, unlike the approach developed by Dorroh which places no restriction on R. However, this extension preserves the characteristic of R and, if R contains an identity element 1_R, then $g(1_R) = \hat{1}_R = i$, the identity in the extension.

§2.5 The Robson-Burgess/Stewart Construction

The Burgess/Stewart approach to extending a ring to a ring with identity was developed as a refinement to the Robson construction.

Lemma 2.5.1 *The ring $K(R)$ is in the center of R, for any ring R with identity.*

Proof. The proof is similar to that used in Lemma 1.2.2, which is found in [DICK 84]. Let I be the ideal of the polynomial ring $R[x]$ generated by x^2. Fix an element $a \in R$ and define functions f, $g : K(R) \longrightarrow R[x]/I$ by $g(k) = k + I$ and $f(k) = (1 + ax)k(1 - ax) + I$ for all $k \in K(R)$. Since $f(1_R) = g(1_R)$ and $K(R)$ is an epimorph of Z, $f(k) = g(k)$ for all k in $K(R)$. Thus, for all k in $K(R)$, $(1 + ax)k(1 - ax) - k$ belongs to I and hence $(ak - ka)x$ is in I. Since I is generated by x^2, $ak = ka$ for all k in $K(R)$. Therefore $K(R) \subseteq Z(R)$. ■

Corollary 2.5.1 *For any ring A, $K(End\, A) = K(End\,_A A_A)$, where $End\,_A A_A$ is the ring of bimodule endomorphisms of A.*

Proof. Since $End\,_A A_A \subseteq End\, A$, $K(End\,_A A_A) \subseteq K(End\, A)$ by Lemma 1.3.2.

Let $\varphi \in K(End\, A)$ and $a \in A$. Since $\varphi \in Z(End\, A)$, $\varphi\hat{a} = \hat{a}\varphi$ and so for any $x \in A$, $(\varphi\hat{a})(x) = (\hat{a}\varphi)(x)$; that is, $\varphi(ax) = a\varphi(x)$. Hence $\varphi \in End\,_A A_A$, and so we have shown that $K(End\, A) \subseteq End\,_A A_A$. Since $K(End\, A)$ is an epimorph of Z, $K(End\, A) \subseteq K(End\,_A A_A)$ as required. ■

Definition 2.5.1 For any ring A, $\hat{K}(A) = K(End\, A)$. □

Let R be a ring with identity. From Proposition 1.3.1 we see that R and $End\, R$ have the same characteristic function, so $K(R) \cong \hat{K}(R)$ by Theorem 1.3.1. In view of this we will refer to $\hat{K}(A)$ as the characteristic ring of A for any ring A.

Example 2.5.1 $\hat{K}(Z_{p^\infty}) \cong Z[1/q \,|\, q \in P \setminus \{p\}]$. *This follows because we already know the characteristic function of Z_{p^∞}.*

Proposition 2.5.1 *Every ring A is a $\hat{K}(A)$-bimodule algebra.*

Proof. Define the action of $\hat{K}(A)$ on A by $\theta \cdot a = a \cdot \theta = \theta(a)$ for all $\theta \in \hat{K}(A)$ and $a \in A$.

Clearly this makes A a left $\hat{K}(A)$-module and also $(a+b)\theta = a\theta + b\theta$, $a1 = a$ and $a(\theta_1 + \theta_2) = a\theta_1 + a\theta_2$ for $a, b \in A$ and $\theta_1, \theta_2, 1 \in \hat{K}(A)$. Also, since $\hat{K}(A)$ is commutative, $a(\theta_1\theta_2) = (\theta_1\theta_2)(a) = (\theta_2\theta_1)(a) = \theta_2(\theta_1(a)) = \theta_1(a) \cdot \theta_2 = (a \cdot \theta_1)\theta_2 = a \cdot (\theta_1\theta_2)$. Hence A is a right $\hat{K}(A)$-module. Further, $\theta_1(a\theta_2) = \theta_1(\theta_2(a)) = \theta_1\theta_2(a) = \theta_2\theta_1(a) = (\theta_1(a))\theta_2 = (\theta_1 \cdot a)\theta_2$ and so A is a $\hat{K}(A)$-bimodule.

We see that the algebra conditions are satisfied, since by Corollary 2.5.1, $\hat{K}(A) \subseteq End_A A_A$, and $(ab)\theta = \theta(ab) = a\theta(b)$ again since $\hat{K}(A) \subseteq End_A A_A$, and so $a \cdot \theta(b) = (a\theta)b = (\theta a)b = \theta(a) \cdot b = \theta(ab) = \theta \cdot (ab)$. Hence A is a $\hat{K}(A)$-bimodule algebra. ■

In view of the above proposition we can imbed any ring A in the Dorroh ring $A \times \hat{K}(A)$, which has an identity. We will denote this ring by A^*.

Proposition 2.5.2 $K(A^*) = \hat{K}(A)$.

Proof. Let g be the characteristic function of $End\,A$. From Propositions 1.3.1 and 1.3.4, A, $K(End\,A)$, A^0 and $(K(End\,A))^0$ all have characteristic function g. By Proposition 1.3.2 $A^0 \times (K(End\,A))^0 = (A \times K(EndA))^0$ also has characteristic function g and so too does $A \times K(EndA)$ by Proposition 1.3.1. Since $K(End\,A)$ is a unital subring of $A \times K(End\,A)$, it follows from Proposition 1.3.5 that $K(A \times K(End\,A)) = K(K(End\,A))$. Hence $K(A^*) = K(EndA) = \hat{K}(A)$. ■

If A is a ring which is left faithful, then $A \cong \hat{A} \subseteq End\,A$. Define $A_1 = \hat{A} + \hat{K}(A)$. Since $\hat{K}(A)$ is in the centre of $End\,A$ by Lemma 2.5.1, A_1 is a subring of $End\,A$ by Lemma 2.4.3 and $\hat{A}$ is an ideal of A_1 which is essential as a right ideal by Lemma 2.4.4.

Proposition 2.5.3 *If A is left faithful, A_1 is a homomorphic image of A^*.*

Proof. Define $\psi : A^* \to A_1$ by $\psi((a,k)) = \hat{a} + k$. It is straightforward to check that ψ is a surjective homomorphism. ■

Proposition 2.5.4 *If A is left faithful, $K(A_1) = \hat{K}(A)$.*

Proof. We have $\hat{K}(A) = K(End\, A) \subseteq A_1 \subseteq End\, A$. Hence by Lemma 1.3.2, $K(\hat{K}(A)) \subseteq K(A_1) \subseteq K(End\, A) = \hat{K}(A)$. Since $K(\hat{K}(A)) = \hat{K}(A)$, the result follows. ■

§2.6 Regular Rings - Fuchs, Halperin and Funayama

Definition 2.6.1 A ring R is regular if, for each x in R, there exists y in R such that $xyx = x$. □

Fuchs and Halperin constructed a commutative regular ring K with identity such that every regular ring R is a K-bimodule algebra. The ring K was then used to construct an extension of any given regular ring R where the extension contains an identity element and is itself regular. This construction is the Dorroh construction where the commutative regular ring K is adjoined to the original ring. The main result of this section is that any regular ring R is isomorphic to a two-sided ideal of a regular ring with identity.

It is interesting to note that no conditions are placed on the ring R other than the requirement that R be regular. We begin by collecting some basic facts about regular rings.

Proposition 2.6.1 *Let R be a regular ring and let $p \in P$.*

1. *If I is an ideal of R, then $I^2 = I$.*

2. *$ann\, t_p(R) = (p^k)$ where $k = 0$ or 1.*

3. pR is p-divisible.

4. $t_p(R) \cap pR = 0$.

5. For each $x \in pR$ *there is a unique* $y \in pR$ *such that* $x = py$.

6. $t_p(R) \oplus pR = R$.

7. If $p_1, \ldots, p_n$ *are distinct primes, then* $R = t_{p_1}(R) \oplus \cdots \oplus t_{p_n}(R) \oplus p_1 \cdots p_n R$ *and* $p_1 \cdots p_n R$ *is divisible by* p_i *for all* $i = 1, \ldots, n$.

8. For each $x \in p_1 \cdots p_n R$ *and each* $i = 1, \ldots, n$ *there is a unique* $y \in p_1 \cdots p_n R$ *such that* $x = p_i y$.

Proof.

1. If $a \in I$, then there is a $b \in R$ such that $a = aba = (ab)a \in I^2$. Hence $I = I^2$.

2. Suppose $m > 1$ and $I = \{x \in R \mid p^m x = 0\}$. Then pI is an ideal of R and $(pI)^m = 0$. Hence $pI = 0$ by 1 above, proving that $ann\, t_p(R) = (p^k)$ where $k = 0$ or 1.

3. Let $a = pb, b \in R$. Then $a = axa$ for some $x \in R$ and so $a = pbxa = p(bxa)$ where $bxa = pbxb \in pR$. Hence pR is p-divisible.

4. Let $a \in t_p(R) \cap pR$. Then $a = pb$ for some b and $pa = 0$ by 2 above. Hence $p^2 b = 0$ and so $pb = 0$, again by 2 above. Thus $a = 0$.

5. Suppose $a = px = py$ where $x, y \in pR$. Then $x - y \in t_p(R) \cap pR$ and hence $x = y$ by 4 above.

6. Let $a \in R$. There is an $x \in R$ such that $pa = (pa)x(pa)$. Thus $a = (a - paxa) + paxa$, $p(a - paxa) = pa - (pa)x(pa) = 0$ and $paxa \in pR$.

7. Let $I = \{a \in R \mid p_1 \cdots p_n a = 0\}$. Clearly $t_{p_i}(R) \subseteq I$ for each $i = 1, \ldots, n$ and the sum $t_{p_1}(R) + \cdots + t_{p_n}(R)$ is direct. Let $\pi_i = (p_1 \cdots p_n)/p_i$, $i = 1, \ldots, n$. Since the p_i are distinct, the greatest common divisor of $\pi_1, \ldots, \pi_n$ is 1. Hence there are integers $\alpha_1, \ldots, \alpha_n$ such that $\alpha_1\pi_1 + \cdots + \alpha_n\pi_n = 1$. So if $a \in I$, then $a = 1 \cdot a = \alpha_1\pi_1 a + \cdots + \alpha_n\pi_n a$ is in $t_{p_1}(R) \oplus \cdots \oplus t_{p_n}(R)$. Thus $t_{p_1}(R) \oplus \cdots \oplus t_{p_n}(R) = I$.

   Let $a \in I \cap p_1 \cdots p_n R$. Then $a = p_1 \cdots p_n x$ for some $x \in R$. Since $a \in I$, $p_1 \cdots p_n a = 0$. Hence $p_1^2 \cdots p_n^2 x = 0$ and so repeated use of result 2 above shows that $p_1 \cdots p_n x = 0$. Hence $a = 0$ and we have $I \cap p_1 \cdots p_n R = 0$. If $a \in R$, $p_1 \cdots p_n a = (p_1 \cdots p_n a)x(p_1 \cdots p_n a)$ for some $x \in R$. Hence $a - p_1 \cdots p_n axa \in I$ and since $a = (a - p_1 \cdots p_n axa) + (p_1 \cdots p_n axa)$ we see that $R = t_{p_1}(R) \oplus \cdots \oplus t_{p_n}(R) \oplus p_1 \cdots p_n R$.

   Let $d = p_1 \cdots p_n x \in p_1 \cdots p_n R$. Because of the direct sum decomposition of R above, $\pi_i x = a_1 + \cdots + a_n + y$ for some $a_i \in t_{p_i}(R)$ and $y \in p_1 \cdots p_n R$. Then $d = p_i\pi_i x = p_i a_1 + \cdots + p_i a_n + p_i y \in p_1 \cdots p_n R$ and so $p_i a_j = 0$ for all j . Hence $d = p_i y$ where $y \in p_1 \cdots p_n R$, so $p_1 \cdots p_n R$ is divisible by p_i for all $i = 1, \ldots, n$.

8. Suppose $x, y, z \in p_1 \cdots p_n R$ and $x = p_i y = p_i z$ for some $i = 1, \ldots, n$. Then $p_i(y - z) = 0$, so $y - z \in t_{p_i}(R) \cap p_1 \cdots p_n R = 0$. Thus $y = z$.

■

Let $p_1, p_2, \ldots, p_n, \ldots$ be an enumeration of the primes and $S = \prod_{i=1}^{\infty} Z/(p_i)$. Denote $K(S)$ by K. Then the elements of K are sequences $\langle u_i \rangle$ such that there is a rational number α/β and $u_i = \bar{\alpha}/\bar{\beta}$ for almost all i.

Proposition 2.6.2 *Every regular ring R is a K-bimodule algebra.*

Proof. Let R be a regular ring and let $a \in R$. Let $\bar{u} = \langle u_i \rangle \in K$. Then there is an $\alpha/\beta \in Q$ and an integer $\bar{M}$ such that $u_i = \bar{\alpha}/\bar{\beta}$ for all $i > \bar{M}$. Choose M

such that $M \geq \bar{M}$ and if p is a prime divisor of β, then $p = p_i$ for some $i \leq M$. From Proposition 2.6.1, $R = t_{p_1}(R) \oplus \cdots \oplus t_{p_M}(R) \oplus p_1 \cdots p_M R$, so we can write $a = a_1 + \cdots + a_M + d$ where $a_i \in t_{p_i}(R)$ and $d \in p_1 \cdots p_M R$. From results 7 and 8 of Proposition 2.6.1 there is a unique $x \in p_1 \cdots p_M R$ such that $d = \beta x$. Define $\bar{u}a = a\bar{u} = u_1 a_1 + \cdots + u_M a_M + \alpha x$.

We now verify that this action is well defined. Suppose H is an integer such that $u_i = \bar{\gamma}/\bar{\delta}$, for some $\gamma/\delta \in Q$, for all $i > H$ and if p is a prime divisor of δ, then $p = p_i$ for some $i \leq H$. Without loss of generality we can assume that $H \geq M$. For all $i > H$, $u_i = \bar{\alpha}/\bar{\beta} = \bar{\gamma}/\bar{\delta}$ and so $\alpha\delta - \beta\gamma$ is divisible by p_i for all $i > H$. Hence $\alpha\delta = \beta\gamma$, so $\alpha/\beta = \gamma/\delta$.

Decompose R as

$$R = t_{p_1}(R) \oplus \cdots \oplus t_{p_H}(R) \oplus p_1 \cdots p_H R \qquad (\star)$$

and write $a = b_1 + \cdots + b_H + \bar{d}$ where $b_i \in t_{p_i}(R)$ for $i = 1, \ldots, H$ and $\bar{d} \in p_1 \cdots p_H R$.

If $y \in R$, $y = c_1 + \cdots + c_H + d'$ for some $c_i \in t_{p_i}(R)$, $i = 1, \ldots, H$, and $d' \in p_1 \cdots p_H R$. Hence $p_1 \cdots p_M y \in t_{p_{M+1}}(R) \oplus \cdots \oplus t_{p_H}(R) \oplus p_1 \cdots p_H R$ because $p_1 \cdots p_M c_i = 0$ for $i \leq M$. So we see that $p_1 \cdots p_M R \subseteq t_{p_{M+1}}(R) \oplus \cdots \oplus t_{p_H}(R) \oplus p_1 \cdots p_H R$.

Let $i \leq M$. Then, since $a = a_1 + \cdots + a_M + d = b_1 + \cdots + b_H + \bar{d}$ and $d \in t_{p_{M+1}}(R) \oplus \cdots \oplus t_{p_H}(R) \oplus p_1 \cdots p_H R$, the fact that the sum $(\star)$ is direct implies that $a_i = b_i$ for $i \leq M$. From this it follows that $d = b_{M+1} + \cdots + b_H + \bar{d}$. Now, for $j \geq M+1$, p_j does not divide β, and so there is a $\bar{b}_j \in t_{p_j}(R)$ such that $b_j = \beta \bar{b}_j$. Also, for $j \geq M+1$, $u_j = \bar{\alpha}/\bar{\beta}$.

Suppose $\bar{x}, \bar{\bar{x}} \in p_1 \cdots p_H R$ are such that $\bar{d} = \beta\bar{x}$ and $\bar{d} = \delta\bar{\bar{x}}$. Note that results 7 and 8 of Proposition 2.6.1 guarantee the existence of $\bar{x}$ and $\bar{\bar{x}}$. Then

$$\begin{aligned} \delta(\gamma\bar{\bar{x}} - \alpha\bar{x}) &= \delta\gamma\bar{\bar{x}} - \delta\alpha\bar{x} \\ &= \delta\gamma\bar{\bar{x}} - \beta\gamma\bar{x} \end{aligned}$$

$$
\begin{aligned}
&= \gamma(\delta\bar{\bar{x}} - \beta\bar{x}) \\
&= \gamma(\bar{d} - \bar{d}) \\
&= 0.
\end{aligned}
$$

Recall that if p is a prime dividing δ, then $p = p_i$ for some $i \leq H$. Hence $\gamma\bar{\bar{x}} - \alpha\bar{x} \in \{r \in R \mid p_1 \cdots p_H r = 0\} = t_{p_1}(R) \oplus \cdots \oplus t_{p_H}(R)$. But $\gamma\bar{\bar{x}} - \alpha\bar{x} \in p_1 \cdots p_H R$, so $\gamma\bar{\bar{x}} - \alpha\bar{x} = 0$.

Now

$$
\begin{aligned}
d &= b_{M+1} + \cdots + b_H + \bar{d} \\
&= \beta\bar{b}_{M+1} + \cdots + \beta\bar{b}_H + \beta\bar{x} \\
&= \beta(\bar{b}_{M+1} + \cdots + \bar{b}_H + \bar{x}).
\end{aligned}
$$

Thus the uniqueness of x implies that $x = \bar{b}_{M+1} + \cdots + \bar{b}_H + \bar{x}$.

The actions of K on R determined by our two decompositions agree on the first M terms because $a_i = b_i$ for $i \leq M$. We now consider the other terms:

$$
\begin{aligned}
v &= u_{M+1}b_{M+1} + \cdots + u_H b_H + \gamma\bar{\bar{x}} \\
&= u_{M+1}\beta\bar{b}_{M+1} + \cdots + u_H\beta\bar{b}_H + \alpha\bar{x} \\
&= \alpha\bar{b}_{M+1} + \cdots + \alpha\bar{b}_H + \alpha\bar{x}
\end{aligned}
$$

since, for $M + 1 \leq i \leq H$, $u_i = \bar{\gamma}/\bar{\delta} = \bar{\alpha}/\bar{\beta}$. Hence $v = \alpha(\bar{b}_{M+1} + \cdots + \bar{b}_H + \bar{x}) = \alpha x$, and so the actions are the same; that is, the action of K on R is well-defined.

It is clear that, with this action, R becomes a unital right and left K-module. Also, the bimodule and algebra conditions are clear because the action is defined "componentwise". Hence R is a K-bimodule algebra. ∎

Let R be a regular ring. In view of Proposition 2.6.2 and the results of Section 2.2, we can form the Dorroh ring $R \times K$ which has ideal $\{(r, 0) \mid r \in R\} \cong R$. We shall show later in Lemma 4.1.5 that K is regular and it will then follow from Lemma 4.1.9 that $R \times K$ is regular. Hence every regular ring can be embedded as a two-sided ideal in a regular ring with identity.

Funayama noted that the ring of bimodule endomorphisms, $\tilde{R}$, of a regular ring R is a commutative regular ring, and used this ring to construct an alternate regular extension of R with identity. Unlike the construction of Fuchs and Halperin which employed the same commutative regular ring K to extend any regular ring R, Funayama's construction employs a ring which depends on R.

Theorem 2.6.1 *If R is a regular ring, then $End_R R_R$ is a commutative regular ring.*

Proof. We first show that $End_R R_R$ is commutative. Let α, β be elements of $End_R R_R$, and let r be an element of R. Let s be the element in R such that $r = rsr$. Then

$$\begin{aligned}
\alpha \circ \beta(r) &= \alpha \circ \beta(rsr) \\
&= \alpha(\beta(r)sr) \\
&= \beta(r)\alpha(s)r \\
&= \beta(r\alpha(s)r) \\
&= \beta \circ \alpha(rsr) \\
&= \beta \circ \alpha(r)
\end{aligned}$$

and so $\alpha\beta = \beta\alpha$, showing that $End_R R_R$ is commutative.

We now demonstrate that $End_R R_R$ is regular. Let $\alpha \in End_R R_R$. We first show that $R = ker\, \alpha \oplus im\, \alpha$.

Let $x \in ker\, \alpha \cap im\, \alpha$. Then $x = \alpha(y)$ for some $y \in R$ and, since $\alpha(x) = 0$, $\alpha^2(y) = 0$. Let $s \in R$ be such that $x = xsx$. Then $x = xsx = \alpha(y)s\alpha(y) = \alpha(\alpha(y)sy) = \alpha(\alpha(y))sy = \alpha^2(y)sy = 0$. Thus $ker\, \alpha \cap im\, \alpha = 0$.

Let $x \in R$ and let v be an element of R such that $\alpha(x) = \alpha(x)v\alpha(x)$. Then $x = (x - \alpha(xvx)) + \alpha(xvx)$ is in $ker\,\alpha + im\,\alpha$. Hence $R = ker\,\alpha \oplus im\alpha$.

Let $x = \alpha(y) \in im\,\alpha$. We will show that there is a unique $z \in im\,\alpha$ such that $x = \alpha(z)$. As above, if $x = xsx$, then $x = \alpha(y)s\alpha(y) = \alpha(\alpha(y)sy) = \alpha(\alpha(ysy))$ and so there is a $z = \alpha(ysy) \in im\,\alpha$ such that $\alpha(z) = x$. Suppose now that z_1, $z_2 \in im\,\alpha$ and $\alpha(z_1) = \alpha(z_2) = x$. Then $z_1 - z_2 \in ker\,\alpha \cap im\,\alpha$ and hence $z_1 = z_2$.

Define $\beta : R \longrightarrow R$ as follows. For $r \in R$, $r = a + b$, where $a \in ker\,\alpha$ and $b = \alpha(c) \in im\,\alpha$ for some unique $c \in im\,\alpha$. Then $\beta(r) = c$. The remarks in the above paragraph and the fact that the sum $ker\,\alpha + im\,\alpha$ is direct guarantee that β is well-defined. Since α is a bimodule endomorphism β is also. Finally, let $x \in R$ and suppose $\alpha(x) = c$ where c is in $im\,\alpha$ and $c = \alpha(d)$, $d \in im\,\alpha$. Then $\alpha\beta\alpha(x) = \alpha\beta(c) = \alpha(d) = c = \alpha(x)$, so $\alpha\beta\alpha = \alpha$. Hence $End_R R_R$ is regular. ■

Proposition 2.6.3 *Let R be a regular ring. Then R is an $End_R R_R$-bimodule algebra.*

Proof. Define the action of $End_R R_R$ on R by $\theta \cdot r = r \cdot \theta = \theta(r)$ for all $\theta \in End_R R_R$ and $r \in R$. Since $End_R R_R$ is commutative, the first part of the proof of Proposition 2.5.1 shows that R is an $End_R R_R$-bimodule. Also, the proof that the algebra conditions are satisfied is as in Proposition 2.5.1. To be explicit, let r, $s \in R$ and $\theta \in End_R R_R$. Then $(\theta r)s = \theta(r) \cdot s = \theta(rs)$, $(r\theta)s = \theta(r)s = \theta(rs)$ and $(rs)\theta = \theta(rs) = r\theta(s)$. ■

In view of this proposition we can form the Dorroh ring $R \times End_R R_R$ which will be regular by Lemma 4.1.9, have an identity and contain a two-sided ideal isomorphic to R.

Recall, from Corollary 2.5.1, that $\hat{K}(R) = K(End_R R_R) \subseteq End_R R_R$. Hence $R^* \subseteq R \times End_R R_R$ and R^* is also a regular ring by Lemmas 4.1.7 and 4.1.9.

An inspection of that part of the proof of Theorem 2.6.1 that shows that $End_R R_R$ is commutative reveals that, for any regular ring R, $\alpha \circ \beta = \beta \circ \alpha$ for any $\alpha \in End_R R_R$ and $\beta \in End\, R$.

Let R be a regular ring. Then the above observation shows that $End_R R_R \subseteq Z(End\, R)$. Also, R is left faithful since if $0 \neq r \in R$ there is an s in R such that $r = rsr$ and hence $rR \neq 0$. As a result we can employ Robson's construction to see that $R \cong \hat{R} \subseteq \hat{R} + End_R R_R$ where $\hat{R} + End_R R_R$ will be regular by Lemma 4.1.9. Also, since $\hat{K}(R) \subseteq End_R R_R$ by Corollary 2.5.1, $R_1 = \hat{R} + \hat{K}(R) \subseteq \hat{R} + End_R R_R$ and R_1 is regular by Corollary 4.1.1.

CHAPTER 3

Universality of the Dorroh Construction

§3.1 The Universal Property

In this chapter we examine universality of the Dorroh construction $R \times Z$ which extends any ring R to a ring with identity. Specifically, we will see that this construction is functorial, and is part of an adjunction. We begin with the universal property, followed by a short discussion on category theory which will provide the background for the last section of this chapter.

In this section we discuss the universal property. Let R be an arbitrary ring and $R \times Z$ be the Dorroh extension of R. Let g be the canonical homomorphism which embeds R into $R \times Z$. We get the following result.

Theorem 3.1.1 *Let T be a ring with identity and f a ring homomorphism, $f : R \longrightarrow T$. Then there is a unique homomorphism $h : R \times Z \longrightarrow T$ preserving the identity such that $h \circ g = f$.*

Proof. We want to show that there is a unique homomorphism h which makes the following diagram commute:

$$\begin{tikzcd}
R \arrow[r, "g"] \arrow[dr, "f"'] & R \times Z \arrow[d, dashed, "\exists ! h"] \\
& T
\end{tikzcd}$$

<u>Existence:</u>

Recall that $g(r) = (r, 0)$. For any integer n let $n_T = n1_T$.

Define $h : R \times Z \longrightarrow T$ by $h(r,n) = f(r) + n_T$. We note that h is a homomorphism since

$$\begin{aligned}
h(r,n) + h(t,m) &= f(r) + n_T + f(t) + m_T \\
&= f(r) + f(t) + n_T + m_T \\
&= f(r+t) + (n+m)_T \\
&= h(r+t, n+m) \\
&= h((r,n) + (t,m)) \\
\text{and } h(r,n)h(t,m) &= (f(r) + n_T)(f(t) + m_T) \\
&= f(r)f(t) + n_T f(t) + m_T f(r) + n_T m_T \\
&= f(rt) + n_T f(t) + m_T f(r) + (nm)_T \\
&= h(rt, 0) + h(nt, 0) + h(mr, 0) + h(0, nm) \\
&= h(rt + nt + mr, nm) \\
&= h((r,n)(t,m))
\end{aligned}$$

for all (r,n), (t,m) in $R \times Z$. We note that h preserves the identity since $h(0,1) = 1_T$.

<u>Uniqueness:</u>

Suppose there exists another homomorphism $h' : R \times Z \longrightarrow T$ preserving the identity such that $h' \circ g = f$. Let (r,n) be in $R \times Z$. By the restrictions placed on h' we must have $h'(r,0) = f(r)$ and $h'(0,n) = n_T$. Therefore $h'(r,n) = h'(r,0) + h'(0,n) = f(r) + n_T = h(r,n)$, so that $h = h'$ proving the theorem. ■

It is noted that the Robson construction of a ring extension does not generally satisfy this universal property. For example, in the case where R has an identity element, the Robson extension of R is $\hat{R} \cong R$. In this case g is the identity map.

Let $T = R \times Z$ be the Dorroh extension of R, with $f : R \longrightarrow R \times Z$ defined as $f(x) = (x, 0)$ for all x in R, so that we have the following situation:

$$\begin{tikzcd} R \arrow[r, "g"] \arrow[dr, "f"'] \arrow[dr, phantom, shift left=4, "///"] & R \arrow[d, dashed, "\exists ! h?"] \\ & R \times Z \end{tikzcd}$$

Then we require a unique map $h : R \longrightarrow R \times Z$ which satisfies $h(1) = (0, 1)$, so $h \circ g(1) = (0, 1)$. However, $f(1) = (1, 0)$, so that $h \circ g \neq f$.

§3.2 Category Theory

In this section we provide the background to category theory required for the discussion in the following section.

Definition 3.2.1 [MACL 71] A <u>category</u> consists of a collection of objects, denoted by $A, B, C, \ldots$ and a collection of morphisms, denoted by $f, g, h, \ldots$ subject to the following:

1) to every morphism, we associate a unique pair of objects called the domain and the codomain. We write $A \xrightarrow{f} B$ and say f is a morphism from A to B;

2) to every object we associate a unique morphism called the identity, and write $A \xrightarrow{1_A} A$;

3) to every pair of morphisms in the situation $A \xrightarrow{f} B \xrightarrow{g} C$ we associate a unique morphism called the composite, and write $A \xrightarrow{g \circ f} C$ (such f and g will be called composable pairs);

4) in the situations $A \xrightarrow{1_A} A \xrightarrow{f} B$ and $A \xrightarrow{f} B \xrightarrow{1_B} B$, we have $f \circ 1_A = f$ and $1_B \circ f = f$; and

5) in the situation $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ we have $h \circ (g \circ f) = (h \circ g) \circ f$.

□

Given a category $\underline{C}$, we denote by $Obj(\underline{C})$ the objects of C and by $Mor(\underline{C})$ the morphisms of C.

An example of a category is $\underline{Rng}$, whose objects are rings and whose morphisms are ring homomorphisms. A second example is $\underline{Ring}$, the category whose objects are rings which contain identity elements and whose morphisms are ring homomorphisms which preserve the identity elements.

Definition 3.2.2 [MACL 71] Given two categories $\underline{C}$ and $\underline{D}$, a <u>functor</u> from $\underline{C}$ to $\underline{D}$, denoted by $\underline{C} \xrightarrow{F} \underline{D}$, associates to each object C of $\underline{C}$ a unique object $F(C)$ of $\underline{D}$ and to each morphism $C \xrightarrow{f} C'$ of $\underline{C}$ a unique morphism $F(C) \xrightarrow{F(f)} F(C')$ of $\underline{D}$ such that $F(1_C) = 1_{F(C)}$ and $F(f \circ g) = F(f) \circ F(g)$ for each composable pair f and g. □

Definition 3.2.3 [MACL 71] A <u>natural transformation</u> between two functors $S, T : \underline{B} \longrightarrow \underline{C}$, denoted by $S \xrightarrow{\tau} T$, assigns to each B in $Obj(\underline{B})$ a unique $SB \xrightarrow{\tau_B} TB$ in $Mor(\underline{C})$ such that for every $B \xrightarrow{f} B'$ in $Mor(\underline{B})$, the following diagram commutes.

$$\begin{tikzcd}
SB \arrow[r, "\tau_B"] \arrow[d, "Sf"'] & TB \arrow[d, "Tf"] \\
SB' \arrow[r, "\tau_{B'}"'] & TB'
\end{tikzcd}$$

□

Definition 3.2.4 [MACL 71] Given two categories $\underline{C}$ and $\underline{D}$ and two functors $\underline{C} \overset{F}{\underset{G}{\rightleftarrows}} \underline{D}$, we say F is a <u>left adjoint</u> of G, denoted $F \dashv G$, if there is a natural transformation $\mu : 1_C \longrightarrow GF$ such that each component $\mu_c : C \longrightarrow GFC$ is universal to G from C (that is, for each morphism $f : C \longrightarrow C'$, $GF(f)$ is the unique morphism h such that $h \circ \mu_C = \mu_{C'} \circ f$. □

§3.3 Adjunction

We next consider some categorical aspects of the Dorroh construction. Specifically, we interpret the Dorroh construction as a functor and as part of an adjunction. The functor $U : \underline{Ring} \longrightarrow \underline{Rng}$, defined by $U(A \xrightarrow{f} B) = A \xrightarrow{f} B$, is commonly called "the forgetful functor", since its action is simply to "forget" the existence of the identity element. The following results are due to [MACL 71].

We define $F : \underline{Rng} \longrightarrow \underline{Ring}$ by $F(A) = A \times Z$ for A in $Obj(\underline{Rng})$ and $F(f)((a,n)) = (f(a), n)$ for $A \xrightarrow{f} B$ in $Mor(\underline{Rng})$.

Proposition 3.3.1 *F is a functor.*

Proof.

There are four conditions which must be satisfied in order for this to be a functor. We have already shown that $F(A) = A \times Z$ is in $Obj(\underline{Ring})$ since $R \times Z$ has an identity element. Let $A \xrightarrow{h} A'$ be in $Mor(\underline{Rng})$. Then $F(h)(a, z) = (h(a), z)$ is in $A' \times Z$. We see that $F(h)$ is a homomorphism which preserves the identity element, since

i) $F(h)(0,1) = (h(0),1) = (0,1)$

ii) $$\begin{aligned} F(h)((a,n)+(b,m)) &= F(h)(a+b,n+m) \\ &= (h(a+b),n+m) \\ &= (h(a)+h(b),n+m) \\ &= (h(a),n)+(h(b),m) \\ &= F(h)(a,n)+F(h)(b,m) \end{aligned}$$

iii) $$\begin{aligned} F(h)((a,n)(b,m)) &= F(h)(ab+nb+ma,nm) \\ &= (h(ab+nb+ma),nm) \\ &= (h(ab)+h(nb)+h(ma),nm) \\ &= (h(ab)+nh(b)+mh(a),nm) \\ &= (h(a)h(b)+nh(b)+mh(a),nm) \\ &= (h(a),n)(h(b),m) \\ &= F(h)(a,n)F(h)(b,m). \end{aligned}$$

For the identity morphisms $A \xrightarrow{i_A} A$ in $\underline{Rng}$ and $A \times Z \xrightarrow{i_{A\times Z}} A \times Z$ in $\underline{Ring}$, we require that $F(i_A) = i_{A\times Z}$. We consider the following diagram:

$$\begin{tikzcd} A \arrow[r, "i_A"] \arrow[d, "F"'] & A \arrow[d, "F"] \\ A \times Z \arrow[r, "i_{FA}"'] & A \times Z \end{tikzcd}$$

We see that $F(i_A)(a,n) = (i_A(a), n) = (a,n) = i_{A\times Z}(a,n)$ for all (a,n) in $A \times Z$.

For any composable pair g and h in $Mor(\underline{Rng})$, we require $F(g \circ h) = F(g) \circ F(h)$. Let $A \xrightarrow{h} A' \xrightarrow{g} A''$ and consider the following diagram.

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[d, "F"'] & A' \arrow[r, "g"] \arrow[d, "F"'] & A'' \arrow[d, "F"] \\ A \times Z \arrow[r, "F(h)"'] & A' \times Z \arrow[r, "F(g)"'] & A'' \times Z \end{tikzcd}$$

Let a be in A and n in Z. Then

$$\begin{aligned} F(g \circ h)(a,n) &= ((g \circ h)(a), n)) \\ &= (g(h(a)), n) \\ &= F(g)(h(a), n) \\ &= F(g)(F(h)(a,n)) \\ &= (F(g) \circ F(h))(a,n) \end{aligned}$$

and therefore $F(g \circ h) = F(g) \circ F(h)$. Thus we see that F is a functor. ■

We note that the functor F gives the Dorroh extension of any ring R.

Proposition 3.3.2 *The functor F is a left adjoint of the functor U.*

Proof. Consider $1_{\underline{Rng}} \xrightarrow{\mu} UF$, where $1_{\underline{Rng}}$ is the identity functor, given at the components by $\mu_A : 1(A) \longrightarrow UF(A)$ where $a \longmapsto (a, 0)$. We note that μ_A is the canonical map (embedding) of Section 2.2. In view of the universality exhibited in Theorem 3.1.1, we need only show naturality. Consider the following square.

$$\begin{tikzcd} A \arrow[r, "\mu_A"] \arrow[d, "h"'] & A \times Z \arrow[d, "UF(h)"] \\ A' \arrow[r, "\mu_{A'}"'] & A' \times Z \end{tikzcd}$$

The top-right composite is $a \longmapsto (a,0) \longmapsto (h(a),0)$. The left-bottom composite is $a \longmapsto h(a) \longmapsto (h(a),0)$. We note that this is similar to the free group construction on a set (being left adjoint to the forgetful functor $\underline{Grp} \longrightarrow \underline{Set}$). We may think of the Dorroh construction as freely providing an identity for R. ■

CHAPTER 4

Properties of the Robson-Burgess/Stewart Construction

§4.1 Properties of R^* and R_1

We now consider properties of the constructions developed in Section 2.5. We recall that R^* is defined as the Dorroh extension of R obtained by adjoining $\hat{K}(R)$ to R. Also, recall that $R_1 = \hat{R} + \hat{K}(R)$, a subring of $EndR$, if R is left faithful.

Lemma 4.1.1 $Z(R^*) = \left\{(r, s) \mid r \in Z(R), s \in \hat{K}(R)\right\}$ *and, if R is left faithful, then* $Z(R_1) = \left\{\hat{r} + s \mid \hat{r} \in Z(\hat{R}), s \in K(\hat{R})\right\}$.

Proof. Let (r, s) and (r_1, s_1) be elements of R^* where r is in $Z(R)$. Then

$$\begin{aligned} (r,s)(r_1,s_1) &= (rr_1 + sr_1 + s_1 r, ss_1) \\ &= (r_1 r + sr_1 + s_1 r, ss_1) \\ &= (r_1, s_1)(r, s). \end{aligned}$$

Therefore $\{(r, s) \mid r \in Z(R)\} \subseteq Z(R^*)$.

Let (r_2, s_2) be in $Z(R^*)$. Then $(r_2, s_2)(r_3, s_3) = (r_3, s_3)(r_2, s_2)$ for all (r_3, s_3) in R^*, so that

$$(r_2r_3 + s_2r_3 + s_3r_2, s_2s_3) = (r_3r_2 + s_3r_2 + s_2r_3, s_2s_3).$$

Thus $r_2r_3 = r_3r_2$. Since r_3 was chosen arbitrarily, we see that r_2 is in $Z(R)$. Therefore $Z(R^*) = \{(r, s) \mid r \in Z(R)\}$.

To prove the second statement, we recall the discussion of Section 2.4 and view R as a subring of $End\ R$, since R is assumed to be left-faithful. We also recall from the discussion in Section 2.5 that the characteristic ring $K(End\ R)$ is contained in $Z(End\ R)$, and $K(End\ R)$ contains the identity of $End\ R$. Since sr is in R for all s in $End\ R$ and all r in R we see that $R_1 = \{r + s \mid r \in R,\ s \in K(End\ R)\}$.

Let $r+s$ be an element of R_1 where r belongs to $Z(R)$. Let r_1+s_1 be an arbitrary element of R_1. Then

$$\begin{aligned}(r+s)(r_1+s_1) &= rr_1+rs_1+sr_1+ss_1\\ &= r_1r+s_1r+r_1s+s_1s\\ &= (r_1+s_1)(r+s).\end{aligned}$$

Therefore we see that $\{r+s \mid r\in Z(R), s\in K(End\ R)\}\subseteq Z(R_1)$. Let $\bar{r}+\bar{s}$ be an element of $Z(R_1)$ where $\bar{r}$ is in R and $\bar{s}$ is in $K(End\ R)$. Then

$$\begin{aligned}(\bar{r}+\bar{s})(r_1+s_1) &= \bar{r}r_1+\bar{r}s_1+\bar{s}r_1+\bar{s}s_1\\ &= \bar{r}r_1+s_1\bar{r}+r_1\bar{s}+s_1\bar{s}\end{aligned}$$

and

$$(r_1+s_1)(\bar{r}+\bar{s}) = r_1\bar{r}+s_1\bar{r}+r_1\bar{s}+s_1\bar{s}.$$

Since $(\bar{r}+\bar{s})(r_1+s_1) = (r_1+s_1)(\bar{r}+\bar{s})$ we see that $\bar{r}r_1 = r_1\bar{r}$. However, r_1 was chosen as an arbitrary element of R, so $\bar{r}$ belongs to $Z(R)$. Thus $Z(R_1) = \{r+s \mid r\in Z(R), s\in K(End\ R)\}$. ■

For the discussion which follows, we require the following definitions.

Definition 4.1.1 Let S be a ring and let $S_1\oplus\cdots\oplus S_k$ be a direct sum of non-zero right ideals of S. If the length of such direct sums is bounded, the right uniform dimension, denoted $\dim S$, is the maximum value of k for the ring S; otherwise S is said to have infinite right uniform dimension. The right uniform dimension of S will be denoted by $dim\, S$. □

Definition 4.1.2 A ring R has the right ascending chain condition if, for any ascending chain of right ideals $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\subseteq\cdots$ there is an integer M such that $I_n = I_M$ for all $n\geq M$. □

Definition 4.1.3 Let X be a subset of a ring S. Then the right annihilator of X in S is $r_s(X) = \{s \in S \mid xs = 0 \text{ for all } x \in X\}$. We note that this is a generalization of Definition 1.3.1. □

Definition 4.1.4 A ring R is a right Goldie ring if R has finite right uniform dimension and the ascending chain condition on right annihilators. □

Definition 4.1.5 *A* ring R is semi-prime if R has no non-zero nilpotent ideals. □

Definition 4.1.6 *A* ring R is prime if, for ideals A and B of R such that $AB = 0$, either $A = 0$ or $B = 0$. □

The following result is due to Andrunakievic.

Lemma 4.1.2 *[DIVI 65] Let C be a ring, B an ideal of C, and A an ideal of B. Let $A^{\ddagger} = A + AC + CA + CAC$ be the ideal of C generated by A. Then ${A^{\ddagger}}^3 \subseteq A$.*

Proof. We see that A, AC, CA, $CAC \subseteq B$ and ${A^{\ddagger}}^3 \subseteq BA^{\ddagger}B$. Thus

$$\begin{aligned} {A^{\ddagger}}^3 \subseteq BA^{\ddagger}B &= B(A + AC + CA + CAC)B \\ &= BAB + BACB + BCAB + BCACB \\ &\subseteq A + AB + BA + BAB \\ &\subseteq A. \end{aligned}$$

■

Lemma 4.1.3 *[ROBS 79] If R is left faithful, then*

i) R is essential as a right ideal of R_1.

ii) R and R_1 have the same right uniform dimension.

iii) R is semi-prime if and only if R_1 is semi-prime.

iv) R is prime if and only if R_1 is prime.

v) [MCCO 87] R is semi-prime Goldie if and only if R_1 is semi-prime Goldie.

Proof. Recall that $R_1 = R + K(End\ R)$ where $K(End\ R)$ is the characteristic ring of *End R*.

i) This follows from Lemma 2.4.4.

ii) We see that $\dim R_1 \geq \dim R$ since $R \subseteq R_1$ and right ideals of R are right ideals of R_1. Thus if $\dim R = \infty$ then $\dim R_1 = \infty$. Suppose $\dim R = k$ for some $k < \infty$, and that $\dim R_1 > \dim R$. Let $\{A_1, A_2, \ldots, A_{k+1}\}$ be a set of right ideals of R_1 such that the sum $A_1 + A_2 + \cdots + A_{k+1}$ is direct. For each $i = 1, 2, \ldots, k+1$, let $B_i = A_i \cap R$, a right ideal of R. Since R is essential as a right ideal of R_1, $B_i \neq 0$ for all i, so $B_1 + \cdots + B_{k+1}$ is a direct sum, a contradiction of our supposition that $\dim R = k$. Therefore $\dim R = \dim R_1$.

iii) Suppose R is semi-prime. If R_1 is not semi-prime, then there is an ideal A of R_1 such that $A \neq 0$ and $A^k = 0$ for some k. Now $A \cap R$ is an ideal of R and $A \cap R \neq 0$ since R is essential as a right ideal of R_1. However $(A \cap R)^k = 0$, a contradiction to the assumption that R is semi-prime. Therefore if R is semi-prime then R_1 is semi-prime.

Conversely, suppose R_1 is semi-prime. If R is not semi-prime then there is an ideal I of R such that $I \neq 0$ and $I^k = 0$ for some k. Let $J = I + IR_1 + R_1 I + R_1 I R_1$, an ideal of R_1. Now, $J \neq 0$ and, in view of Lemma 4.1.2, we see that $J^3 \subseteq I$, so $J^{3k} = 0$, showing that R_1 is not semi-prime, a contradiction. Therefore if R_1 is semi-prime then R is semi-prime.

iv) Suppose R_1 is prime. Recall that R is viewed as a subring of $End(R)$ and R is an ideal of R_1. Let A and B be ideals of R such that $AB = 0$. Let $A^* = A + AR_1 + R_1A + R_1AR_1$ and let $B^* = B + BR_1 + R_1B + R_1BR_1$. From Lemma 4.1.2 we see that both A^* and B^* are ideals of R_1 such that $A^{*^3} \subseteq A$ and $B^{*^3} \subseteq B$. Since $AB = 0$ we see that $A^{*^3}B^{*^3} = 0$. Since R_1 is prime we have that either $A^* = 0$ or $B^* = 0$. Now $A \subseteq A^*$ and $B \subseteq B^*$, so that either $A = 0$ or $B = 0$. Thus either $A = 0$ or $B = 0$, proving that R is prime.

Conversely, suppose R is prime. Let A and B be ideals of R_1 such that $AB = 0$. Now $A \cap R$ and $B \cap R$ are ideals of R such that $(A \cap R)(B \cap R) = 0$. Thus either $A \cap R = 0$ or $B \cap R = 0$ since R is prime. Therefore either $A = 0$ or $B = 0$ because R is essential as a right ideal of R_1, and so R_1 is prime.

v) We have already shown that R is semi-prime if and only if R_1 is semi-prime, and that R and R_1 have the same right uniform dimension. It remains then to show that R has the ascending chain condition on right annihilators (denoted ACCRA) if and only if R_1 has the ACCRA.

Suppose that R has the ACCRA and let $X_i \subseteq R_1$, for $i = 1, 2, \ldots$ be subsets of R_1 such that $r_{R_1}(X_1) \subseteq r_{R_1}(X_2) \subseteq \cdots \subseteq r_{R_1}(X_n) \subseteq \cdots$ is an ascending chain of right annihilators in R_1.

Let $a \in R$. For each i, if $X_ia = 0$ then $RX_ia = 0$. Assume that $RX_ia = 0$. Then $X_ia = 0$, for otherwise $RSR + RS + SR + S$, where S is the subring of R generated by X_ia, would be a non-zero nilpotent ideal of the semi-prime ring R, a contradiction. Thus $X_ia = 0$ if and only if $RX_ia = 0$.

Consequently we see that

$$r_{R_1}(X_i) \cap R = \{a \in R \mid ra = 0 \text{ for all } r \in X_i\} = r_R(RX_i).$$

Thus we have an ascending chain of right annihilators in R,

$$r_R(RX_1) \subseteq r_R(RX_2) \subseteq \cdots \subseteq r_R(X_n) \subseteq \cdots$$

which must terminate since R is assumed to have ACCRA. So there exists an integer M such that $r_R(RX_M) = r_{R_1}(RX_n)$ for all $n \geq M$. Fix some integer t where $t \geq M$. We must show that $r_{R_1}(X_t) = r_{R_1}(X_M)$, and since $r_{R_1}(X_M) \subseteq r_{R_1}(X_t)$ we need only show $r_{R_1}(X_t) \subseteq r_{R_1}(X_M)$.

If $\beta R = 0$ for some $\beta \in R_1$, then $\beta = 0$. To show this, let $I = \{\beta \in R_1 \mid \beta R = 0\}$, an ideal of R_1. If $I \neq 0$ then $I \cap R \neq 0$ since R is essential as a right ideal of R_1. Therefore $(I \cap R)^2 = 0$, a contradiction of the assumption that R is semi-prime. Thus $I = 0$. Similarly we see that if $R\beta = 0$ then $\beta = 0$.

Now, suppose $X_t\alpha = 0$ for some $\alpha \in R_1$. Then $X_t\alpha R = 0$ so that $\alpha R \subseteq r_R(RX_t) = r_R(RX_M)$. Thus $RX_M\alpha R = 0$, and so $RX_M\alpha = 0$ since R is left faithful, and thus $X_M\alpha = 0$, showing that $\alpha \in r_{R_1}(X_M)$. Therefore $r_{R_1}(X_t) \subseteq r_{R_1}(X_M)$, proving that R_1 has ACCRA if R has ACCRA.

It remains to show that if R_1 has ACCRA then R has ACCRA.

Suppose R_1 has ACCRA and let $X_i \subseteq R$ for $i = 1, 2, \ldots$ be subsets such that $r_R(X_1) \subseteq r_R(X_2) \subseteq \cdots \subseteq r_R(X_n) \subseteq \cdots$ is an ascending chain of right annihilators in R. Let $Y_i = \cup_{j=i}^{\infty} X_i$ for each i. Then $r_R(Y_i) \subseteq r_R(Y_{i+1})$ for all i and $r_R(X_i) = r_R(Y_i)$ for all i.

Since $Y_{i+1} \subseteq Y_i$ for all i, $r_{R_1}(Y_1) \subseteq r_{R_1}(Y_2) \subseteq \cdots \subseteq r_{R_1}(X_n) \subseteq \cdots$ is an ascending chain of right annihilators in R_1. Thus there is an integer $\bar{M}$ such that $r_{R_1}(Y_{\bar{M}}) = r_{R_1}(Y_i)$ for all $i \geq \bar{M}$. Since for all i, $r_R(Y_i) = R \cap r_{R_1}(Y_i)$ and $r_R(Y_i) = r_R(X_i)$, it follows that $r_R(X_{\bar{M}}) = r_R(X_i)$ for all $i \geq \bar{M}$.

■

Definition 4.1.7 A ring R is right noetherian if, for any ascending chain of right ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$, there is an integer M such that $I_n = I_M$ for all $n \geq M$. □

Definition 4.1.8 A ring T is right artinian if, for any descending chain of right ideals $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$, there is an integer M such that $I_n = I_M$ for all $n \geq M$. Left artinian is similarly defined. A ring T is artinian if it is both left and right artinian. □

Lemma 4.1.4 *Let R be a ring and K an ideal of R. Then:*

i) if R/K and K are right artinian, then R is right artinian; and

ii) if R/K and K are right noetherian, then R is right noetherian.

Proof.

i) Let $\{I_n\}$ for $n \geq 1$, be a decreasing chain of right ideals of R. Then $\{(I_n+K)/K\}$ is a decreasing chain of right ideals of R/K, so there exists an integer M_1 such that $(I_n + K)/K = (I_{M_1} + K)/K$ for all $n \geq M_1$. Similarly, $\{I_n \cap K\}$ is a decreasing chain of right ideals of K, so there exists an integer M_2 such that $I_n \cap K = I_{M_2} \cap K$ for all $n \geq M_2$. Let M be the greater of M_1 and M_2. Fix n such that $n \geq M$. Let $x \in I_M$. Then $x + K = r + K$ for some $r \in I_n$ so $x = r + k$ for some $k \in K$. Now $x - r = k \in I_M$ and $x - r = k \in K$, so $k \in I_M \cap K$. Therefore $k \in I_n \cap K$. Thus $x = r + k \in I_n$. So $I_M \subseteq I_n$, showing that $I_M = I_n$.

ii) The proof for right noetherian rings is similar.

■

Recall from Example 1.3.1 the definition of a quasi-cyclic group, Z_{p^∞}, for any prime p. It is interesting to note that the only proper subgroups of Z_{p^∞} are generated by $1/p^n$ for any n. Consequently, we see that quasi-cyclic groups are artinian, but are not noetherian.

The following result is due to Fuchs, and is stated without proof.

Theorem 4.1.1 *[FUCH 60] An artinian ring U, with no additive subgroup which is a quasi-cyclic group, is the ring-theoretic direct sum of a torsion free artinian ring B and a finite number of artinian p-rings C_i belonging to the different primes p_i,*

$$U = B \oplus C_1 \oplus \cdots \oplus C_r.$$

The rings B, C_1, ... , C_r are uniquely determined.

Proposition 4.1.1 *[BURG 89]*

i) If R is right noetherian, so are R^* and R_1;

ii) If R is right artinian and R has no additive subgroup which is a quasi-cyclic group, then R^* and R_1 are right artinian.

Proof.

i) We note that R is an ideal of both R^* and R_1. Since R is assumed to be right noetherian we need only show that $K(R)$ is right noetherian since $K(R) \simeq R_1/R$ and $K(R) \simeq R^*/R$; Lemma 4.1.4 will then complete the proof.

Suppose $K(R)$ is of form C. Then $K(R)$ is not noetherian, as the ascending chain of ideals $\{\prod_{i=1}^{n} Z/(p_i^{\alpha_i})\}$ shows. Thus R is not right noetherian, since $\{I_n = \oplus_{i=1}^{n} t_{p_i}(R)\}$ is a set of ideals of R such that $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ and for each n there exists an $n' > n$ such that $I_n \neq I_{n'}$, a contradiction. Therefore $K(R)$ is either of form A or B, both of which are right noetherian. Thus R^* and R' are right noetherian.

ii) From Theorem 4.1.1 we see that $K(R)$ is either of form A, or of form B where D is a right artinian ring (if $R = Q$, X_0 is infinite). Thus $K(R)$ is right artinian, and the result follows from Lemma 4.1.4.

■

We recall Example 1.3.1 and note the case of $R = Z_{p^\infty}$, which is right artinian and has $K(Z_{p^\infty}) = Z[1/q \mid q \neq p]$. Since $K(Z_{p^\infty})$ is not right artinian, R^* and R_1 are not right artinian. This example shows the necessity of R not containing an additive subgroup which is quasi-cyclic if the right artinian property is to be extended from R to R^* and R_1.

Definition 4.1.9

a) An element $e \in R$ is an <u>idempotent</u> if $e^2 = e$.

b) Let I be an ideal of R. I is <u>idempotent</u> if $I^2 = I$.

c) R is <u>strongly regular</u> if, for each x in R, there exists y in R such that $x^2y = x$.

d) An element e in R is <u>central</u> if $ex = xe$ for all x in R.

e) For each element a in R let (a) denote the principal ideal generated by a. The ring R is <u>biregular</u> if for each a in R there exists a central idempotent e in R such that $(a) = (e)$.

□

For the rest of this section all rings are assumed to have all ideals idempotent and hence are left-faithful.

Lemma 4.1.5 *Let R be such that every ideal is idempotent. Then $K(R)$ is regular.*

Proof. We note that, in the case where $K(R) = Z/I$ for some non-zero ideal I of Z, $K(R)$ must be a finite direct sum of fields and so $K(R)$ is regular. Thus the remainder of the proof will consider the case where $K(R)$ is either of form B or form C. Let $f : P \longrightarrow N \cup \{\infty\}$ denote the function which determines $K(R)$, $X_1 = \{p \in P \mid 0 < f(p) < \infty\}$, $X_0 = \{p \in P \mid 0 \leq f(p) < \infty\}$ and $D = Z[X_0^{-1}]$.

Let p be a prime number. Then

$$pR = (pR)^2 = pRpR = (p^2)(R^2) = p(pR)$$

since pR is an ideal of R. Hence pR is p-divisible.

Recall that $t_p(R) = \{x \in R \mid p^n x = 0 \text{ for some } n \geq 1\}$. Then

$$pt_p(R) = (pt_p(R))^2 = p^2(t_p(R))^2 = p^2 t_p(R)$$

since $t_p(R)^2 = t_p(R)$.

Therefore,

$$pt_p(R) = p(pt_p(R)) = p(p^2 t_p(R)) = p^2(pt_p(R)) = \cdots = p^m t_p(R).$$

If x is in $t_p(R)$, $p^m x = 0$ for some $m \geq 1$, and hence

$$xpt_p(R) = xp^m t_p(R) = p^m x t_p(R) = 0 t_p(R) = 0.$$

Hence, $t_p(R)(pt_p(R)) = 0$, so $(pt_p(R))^2 = 0$. Therefore $pt_p(R) = 0$ since $pt_p(R) = (pt_p(R))^2$. Consequently, $ann\, t_p(R) = (p^k)$ for $k = 0$ or 1.

We will show that $R = pR \oplus t_p(R)$. Let a be an element of R. Since $pR = p^2 R$ there is an element b in R such that $pa = p^2 b$. Hence $p(a - pb) = 0$ and so $a - pb$ is an element of $t_p(R)$. Now, $a = pb + (a - pb)$ which is contained in $pR + t_p(R)$, so $R = pR + t_p(R)$. Also, since pR is p-divisible and $pt_p(R) = 0$, $pR \cap t_p(R) = 0$. Hence $R = pR \oplus t_p(R)$ and so $f(p) = 0$ or 1 and $D = Z[X_0^{-1}] = Q$.

Recall that X_1 is the set of primes p_i for which a component $Z/(p_i^{n_i})$, for some integer $n_i \geq 1$, appears.

If X_1 is finite, so that $K(R) \simeq Q \oplus Z/(p_1) \oplus \cdots \oplus Z/(p_n)$, then $K(R)$ is regular because it is isomorphic to a direct sum of fields. On the other hand, if X_1 is infinite then $K(R) \simeq \{\langle u_i\rangle \mid \langle u_i\rangle$ is an element of $\prod_{p\in X_1} Z/(p)$ such that there is some a/b in Q and $u_i = \bar{a}/\bar{b}$ for almost all $i\}$. Let $\langle u_i\rangle$ be an element of $K(R)$. Define the components of $\langle v_i\rangle$ by:

$$v_i = \begin{cases} u_i^{(-1)} & \text{if } u_i \neq 0 \\ 0 & \text{if } u_i = 0. \end{cases}$$

Then $\langle v_i\rangle$ is also an element of $K(R)$ and $\langle u_i\rangle\langle v_i\rangle\langle u_i\rangle = \langle u_i\rangle$. Hence $K(R)$ is regular. ■

Lemma 4.1.6 *Let R be strongly regular. Then $K(R)$ is strongly regular.*

Proof. If R is strongly regular, then all ideals of R are idempotent. Consequently, by Lemma 4.1.5 $K(R)$ is regular. Since $K(R)$ is also commutative, $K(R)$ is strongly regular. ■

Lemma 4.1.7 *Let R be regular. Then $K(R)$ is regular.*

Proof. From Proposition 2.6.1 we see that all ideals of R are idempotent. Therefore $K(R)$ is regular. ■

Lemma 4.1.8 *$K(R)$ is regular if and only if $K(R)$ is strongly regular.*

Proof. We note that $K(R)$ is commutative, since it is an epimorph of Z. ■

Lemma 4.1.9 *Let A be a ring, B an ideal of A. If A/B and B are both regular, then A is regular.*

Proof. Let a be an element of A. There exists an element $x \in A$ such that $(a+B)(x+B)(a+B) = (a+B)$ since A/B is regular. Thus $axa + B = a + B$, so $axa - a$ is an element of B. Since B is regular, there exists an element b of B such that $(axa-a)b(axa-a) = axa - a$. Therefore $a(xab + bax - xabax - b + x)a = a$ as desired. ∎

Corollary 4.1.1 *If R is regular then R_1 is regular.*

Proof. Since $K(R) \simeq R_1/R$ and $K(R)$ is regular the conditions of the lemma apply, showing that R_1 is regular. ∎

Lemma 4.1.10 *Let A be a ring, B an ideal of A. If A/B and B are both strongly regular, then A is strongly regular.*

Proof. Let a be an element of A. There exists an element $x \in A$ such that $(a+B)^2(x+B) = a + B$ since A/B is strongly regular. Thus $a^2x - a$ is an element of B. Since B is strongly regular there exists an element b in B such that $(a^2x - a)(a^2x - a)b = a^2x - a$, and so $a = a^2(x - xa^2xb + xab + axb - b)$, proving that A is strongly regular. ∎

Corollary 4.1.2 *If R is strongly regular then R_1 is strongly regular.*

Proof. Since $K(R) \simeq R_1/R$ is strongly regular by Lemma 4.1.6, R_1 is strongly regular. ∎

Lemma 4.1.11 *Let A be a ring with identity, B an ideal of A. If B has all ideals idempotent and A/B is commutative regular, then A has all ideals idempotent.*

Proof. Let I be an ideal of A, and let a be an element of I. Then $(I+B)/B$ is an ideal of A/B, which is commutative regular. Thus there exists an element b in A such that $(a+B)^2(b+B) = a+B$. Therefore a^2b-a is an element of B. Let J be the ideal of B generated by a^2b-a. Now $J=J^2$ and $J \subseteq I$, so $J = J^2 \subseteq I^2$. Hence $(a^2b-a) \in I^2$ and since $a^2b \in I^2$, $a \in I^2$. This shows that $I \subseteq I^2$ and so all ideals of A are idempotent. ■

Corollary 4.1.3 *If R has all ideals idempotent then R_1 has all ideals idempotent.*

Proof. We note that $K(R) \simeq R_1/R$ is commutative regular by Lemma 4.1.5. ■

Finally, we show that the Burgess/Stewart extension of a biregular ring is also biregular and so every biregular ring can be embedded in a biregular ring with identity. This result is due to [VRAB 70]. To demonstrate this we first require the following definitions.

Definition 4.1.10 The Boolean algebra of central idempotents of a ring $(S,+,\cdot)$ is $(B,\bar{+},*)$ where $B=\{e \in Z(S) \mid e\cdot e = e\}$ and the operations are defined by

$$e\bar{+}f = e+f-2e\cdot f \quad \text{and} \quad e*f = e\cdot f$$

□

Lemma 4.1.12 *The Boolean algebra of any ring S is an associative ring.*

Proof.

The proof involves a straight forward check of the ring properties. Let e,f,g be in B and s in S. Then

$$(e*f)\cdot(e*f) = e\cdot f\cdot e\cdot f = e\cdot e\cdot f\cdot f = e\cdot f = e*f,$$

We also note that

$$(e * f) \cdot s = e \cdot f \cdot s = e \cdot s \cdot f = s \cdot e \cdot f = s \cdot (e * f),$$

and

$$\begin{aligned}
(e \bar{+} f) \cdot (e \bar{+} f) &= (e + f - 2e \cdot f) \cdot (e + f - 2e \cdot f) \\
&= e \cdot e + e \cdot f - 2e \cdot f \cdot e + f \cdot e + f \cdot f - f \cdot 2e \cdot f - 2e \cdot f \cdot e \\
&- 2e \cdot f \cdot f + 2 \cdot e \cdot f \cdot 2e \cdot f \\
&= e + e \cdot f - 2e \cdot f + e \cdot f + f - 2e \cdot f - 2e \cdot f - 2e \cdot f + 4e \cdot f \\
&= e + f - 2e \cdot f \\
&= (e \bar{+} f)
\end{aligned}$$

and

$$\begin{aligned}
(e \bar{+} f) \cdot s &= (e + f - 2e \cdot f) \cdot s \\
&= e \cdot s + f \cdot s - 2e \cdot f \cdot s \\
&= s \cdot e + s \cdot f - s \cdot 2e \cdot f \\
&= s \cdot (e \bar{+} f).
\end{aligned}$$

Thus $e * f$ and $e \bar{+} f$ belong to B.

We see that $\bar{+}$ is associative since

$$\begin{aligned}
(e \bar{+} f) \bar{+} g &= (e + f - 2e \cdot f) \bar{+} g \\
&= e + f - 2 \cdot e \cdot f + g - 2 \cdot (e + f - 2e \cdot f) \cdot g \\
&= e + f - 2e \cdot f + g - 2e - 2f - 4e \cdot f \cdot g \\
&= e + f + g - 2f \cdot g - 2e \cdot f - 2e \cdot g + 4e \cdot f \cdot g \\
&= e + (f + g - 2f \cdot g) - 2e \cdot (f + g - 2fg) \\
&= e \bar{+} (f + g - 2f \cdot g) \\
&= e \bar{+} (f \bar{+} g).
\end{aligned}$$

We also note that

$$e\bar{+}f = e + f - 2e \cdot f = f + e - 2f \cdot e = f\bar{+}e$$

and

$$e\bar{+}0 = e,$$

so that $\bar{+}$ is commutative and has an additive identity. We see that elements of B have additive inverses since $e\bar{+}e = e + e - 2e \cdot e = 0$. Finally, we see that B satisfies the distributive property since

$$\begin{aligned} e * (f\bar{+}g) &= e * (f + g - 2f \cdot g) \\ &= e \cdot f + e \cdot g - 2e \cdot f \cdot g \\ &= e \cdot f + e \cdot g - 2e \cdot f \cdot e \cdot g \\ &= e \cdot f\bar{+}e \cdot g \\ &= (e * f)\bar{+}(e * g). \end{aligned}$$

Thus $(B, \bar{+}, *)$ is an associative ring. ∎

We require the following three lemmas which will be used to prove that the Burgess/Stewart extension preserves biregularity.

Lemma 4.1.13 *Let S be a ring with identity and B the Boolean algebra of central idempotents of S. If N is a maximal ideal of S then $(N \cap B)$ is a maximal ideal of B.*

Proof. Let e, f be in $N \cap B$ and g be in B. Then $e\bar{+}f = e + f - 2ef$ belongs to $N \cap B$ and $g * e = ge$ is in $N \cap B$, so $N \cap B$ is an ideal of B. Let I be an ideal of B containing $N \cap B$ where $N \cap B \neq I$. Let e be in $I \backslash N \cap B$. Then $N + eS = S$ since N is a maximal ideal of S, so $1 = n + es$ for some n in N and s in S. Therefore

$e = en + es$, so $1 - e = n - en$ belongs to N. Thus $1 - e$ belongs to $N \cap B$, which is contained in I, so $e \bar{+} (1 - e)$ belongs to I. Since

$$\begin{aligned} e \bar{+} (1-e) &= e + 1 - e - 2e(1-e) \\ &= 1 - 2(e - e^2) \\ &= 1 \end{aligned}$$

we see that 1 belongs to I, and so $I = B$. Therefore $N \cap B$ is a maximal ideal of B. ∎

Lemma 4.1.14 *Let S be a ring and B the Boolean algebra of central idempotents of S. If e, f are elements of B then $u = e + f - ef$ is in B and $eu = e$, $fu = f$. If I is an ideal of S then $I \cap B$ is an ideal of B. If I is an ideal of S and $C = I \cap B$ then CS is an ideal of S and for any element x in CS there are elements e in C and s in S such that $x = es$.*

Proof. Let e, f be elements of B, s an element of S and $u = e + f - ef$. Then

$$\begin{aligned} u^2 &= (e+f-ef)(e+f-ef) \\ &= ee + ef - eef + fe + ff - fef - efe - eff + efef \\ &= e + ef - ef + ef + f - ef - ef - ef + ef \\ &= e + f - ef \\ &= u \end{aligned}$$

and

$$\begin{aligned} us &= (e+f-ef)s \\ &= es + fs - efs \\ &= se + sf - sef \\ &= su \end{aligned}$$

so u belongs to B. We also note that

$$\begin{aligned} eu &= e(e+f-ef) \\ &= e^2+ef-e^2f \\ &= e \end{aligned}$$

and similarly $fu = f$, proving the first statement.

Now, let I be an ideal of S, g an element of B and e, f elements of $I \cap B$. Then $e\bar{+}f = e + f - ef$ is in I, and so $e\bar{+}f$ belongs to $I \cap B$. Also, $e * g = eg$ is in I, so $e * g$ is in $I \cap B$. Thus $I \cap B$ is an ideal of B, verifying the second statement.

Finally, we verify the third statement. Let I be an ideal of S and $C = I \cap B$. Let $x = \sum_{i=1}^{n} e_i s_i$ be an element of CS for some positive integer n and elements e_i in C and s_i in S. Suppose $n = 2$, so that $x = e_1s_1 + e_2s_2$. Let $u = e_1 + e_2 - e_1e_2$. Then $ue_1 = e_1$ and $ue_2 = e_2$ so that $x = u(e_1s_1 + e_2s_2)$ is of the required form since u is in C. We assume that if $x = \sum_{i=1}^{n-1} e_i s_i$ then $x = es$ for some e in S and s in S.

Now suppose $x = \sum_{i=1}^{n} e_i s_i$. Then $x = \sum_{i=1}^{n-1} e_i s_i + e_n s_n$ so that $x = \bar{e}\bar{s} + e_n s_n$ for some $\bar{e}$ in C and $\bar{s}$ in S. As above, let $\bar{u} = \bar{e} + e_n - \bar{e}e_n$. Then $x = \bar{u}(\bar{e}\bar{s} + e_n s_n)$ is of the right form. Thus, by induction on n, we see that for any x in CS there are elements e in C and s in S such that $x = es$.

Now suppose e_1s_1 and e_2s_2 are elements of CS. Then $e_1s_1 + e_2s_2 = us$ for some u in C and s in S. Also, for any s' in S we see that $(e_1s_1)s' = e_1(s_1s')$ is in CS and $s'(e_1s_1) = (s'e_1)s_1 = (e_1s')s_1 = e_1(s's_1)$ is in CS. Thus CS is an ideal of S. ■

Lemma 4.1.15 *If S is a semiprime ring with identity such that, for every maximal ideal M of B, the Boolean ring of central idempotents of S, MS is a maximal ideal of S then S is biregular.*

Proof. Let a be a non-zero element of S and (a) the principal ideal of S generated by a. Since S contains an identity we see that $(a) = SaS$. We first show that $S =$

$SaS \oplus lann\, SaS$ where $lann$ denotes the left annihilator in S. Let $I = SaS \cap lann\, SaS$, an ideal of S. Then $I^2 = 0$ so $I = 0$ since S is semiprime. Suppose $SaS \oplus lann\, SaS$ is a proper ideal of S. Since S has an identity, we see that $SaS \oplus lann\, SaS$ is a contained in some maximal ideal N of S by Zorn's lemma. From Lemma 4.1.13 we note that $N \cap B$ is a maximal ideal of B. Thus, by assumption, $(N \cap B)S$ is a maximal ideal of S. Now $(N \cap B)S$ is contained in N, so $(N \cap B)S = N$. Since a is in N, $a = es$ for some e in $N \cap B$ and some s in S by Lemma 4.1.14. Further, $(1-e)SaS = S(1-e)esS = S \cdot 0 \cdot S = 0$, so $1-e$ belongs to $lann\, SaS$, and thus $1-e$ is in N. Therefore $1 = (1-e) + e$ is in N contradicting the supposition that $N \neq S$. Therefore $S = SaS \oplus lann\, SaS$.

Let $1 = e + f$ where e is in SaS and f belongs to $lann\, SaS$. Let x be in SaS. Then $ex - x = (1-f)x - x = -fx$ is in $lann\, SaS$. Since $ex - x$ is also in SaS and $SaS \cap lann\, SaS = 0$, we see that $ex = x$. Thus $e^2 = e$ and $SaS = SeS$. For any s in S, $es - se = (1-f)s - s(1-f) = -fs + sf$ and so, as above, $es = se$ showing that e is central, and showing that S is biregular. ■

We next show that certain extensions of biregular rings are biregular, from which the preservation of biregularity by the Burgess/Stewart construction will follow.

Lemma 4.1.16 *Suppose S is a ring with identity containing an ideal R which, as a ring, is biregular. Also, suppose S has a central regular subring T such that $S = R + T$. Then S is biregular.*

Proof. We note that both R and T are semiprime. Let I be an ideal of S such that $I^2 = 0$. Now S/R is semiprime since

$$\frac{S}{R} = \frac{T+R}{R} \simeq \frac{T}{T \cap R},$$

which is regular since homomorphic images of regular rings are regular. Since

$$\frac{I+R}{R} \subseteq \frac{S}{R}$$

we see that $I \subseteq R$. Thus $I = 0$ since R is biregular. Therefore S is semiprime.

Let B be the Boolean algebra of central idempotents of S, and M a maximal ideal of B. By Lemma 4.1.15 it suffices to show that MS is a maximal ideal of S. We note that since $S = R + T$ and T is central, central idempotents of R are in B.

Suppose that there exists an ideal K of S containing MS and $K \neq MS$. We need to show that $K = S$. There are three cases to consider.

Case I: If $MS \cap R \neq K \cap R$ there is, since R is biregular, a central idempotent e of R such that e is in $K \cap R$ and e does not belong to $MS \cap R$. As noted above, e is in B, so e is not in M and thus $1 = e \bar{+} m$ for some m in M. Therefore $1 = e + m - 2em$ and hence $1 - e$ is in MS. Thus e, $1 - e$ belong to K and so $K = S$, proving that S is biregular.

Case II: If $MS \cap R = K \cap R$ and R is contained in MS, then $R \subseteq MS \subset K$ and

$$\begin{aligned} K &= K \cap S \\ &= K \cap (R + T) \\ &= K \cap (MS + T) \\ &= MS + K \cap T \ \text{ (since } MS \subseteq K). \end{aligned}$$

Since $MS \neq K$ there is a non-zero element s in $K \cap T$ such that s is not in MS. There is an element t in T such that $s = sts$, since T is regular, and so $e = st$ is an idempotent. We note that e is not in MS since $s = es$ and s is not in MS. Further, e is in B since e belongs to T and T is central. We note that e is not in M since e is not in MS, so $1 - e$ belongs to M, as discussed above. Thus e, $1 - e$ belong to K and so $K = S$. Hence S is biregular.

Case III: Suppose $MS \cap R = K \cap R$ and R is not contained in MS. Let a be an element in R where a is not in MS. There is a central idempotent e in R such that

$(a) = (e)$, since R is biregular. As noted above, e is in B. Since a is not in MS, neither is e in MS. Thus e is not in M and, as above, $1 - e$ is in M. Therefore both e and $1 - e$ are in $MS + R$, so $MS + R = S$.

Let k be an element of K. Then there exist elements x in MS and r in R such that $k = x + r$. Thus $k - x = r$ is in $K \cap R$, since MS is contained in K. Further, $k - x = r$ is in MS since $K \cap R = MS \cap R$. Thus $k = x + r$ is in MS and so K is contained in MS, contradicting our assumption that K is a proper extension of MS. Therefore this case III can not occur.

■

Corollary 4.1.4 *If R is biregular then R^* and R_1 are biregular.*

Proof. Since every ideal of R is idempotent, $K(R)$ is regular by Lemma 4.1.5. ■

CHAPTER 5

Conclusion

We have considered a variety of methods which extend any given ring to a ring with identity, although some methods are restricted in regard to the rings which may be extended. For instance, the method developed in [ROBS 79], and by implication the refinements made by [BURG 89], requires that the given ring be left-faithful, while the methods discussed in [FUCH 68, FUNA 66] deal only with regular rings.

We have shown that the construction given by [DORR 32] extends any ring to a ring with identity by adjoining the ring of integers to the original ring. While this approach places no restrictions on the original ring, many of the properties of the original ring may be lost in the extension. However, this construction is functorial, and in fact is part of an adjunction.

The method discussed in [ROBS 79] embeds the original ring R (which is required to be left-faithful) into the ring of endomorphisms of R, which contains an identity. More generally, we see that $R + C$ is an extension of R with identity for any subring C of the center of *End* R.

[BURG 89] refines the method developed in [ROBS 79] by adjoining the characteristic ring to the original ring. We have shown that this construction retains many of the properties possessed by the original ring.

In the case of regular rings, we have shown that there is a commutative regular ring with identity S such that every regular ring is an S-bimodule. This ring was used in [FUCH 68] to develop a construction which extends any regular ring to a regular ring with identity. A second construction regarding regular rings was developed in [FUNA 66] by adjoining to a regular ring R the ring of endomorphism of R, using arithmetic similar to that used by [DORR 32]. In view of the method discussed in [ROBS 79], we have suggested a refinement to Funayama's approach.

Bibliography

[BROW 46] B. Brown and N. McCoy, "Rings with Unit Element which Contain a Given Ring", Duke Math. J. 13 (1946) 9-20.

[BURG 89] W.D. Burgess and P.N. Stewart, "The Characteristic Ring and the Best Way to Adjoin a One", J. Australian Math. Soc. (Series A) 47 (1989) 483-496.

[CHEA 72] T. Cheatham and E. Enochs, "The Epimorphic Images of a Dedekind Domain", Proc. Amer. Math. Soc. 35 (1972) 37-42.

[DICK 84] W. Dicks and W. Stephenson, "Epimorphs and Dominions of Dedekind Domains", J. London Math. Soc. 29 (1984) 224-228.

[DIVI 65] N. J. Divinsky, Rings and Radicals, (University of Toronto Press, Toronto, 1965).

[DORR 32] J.L. Dorroh, "Concerning Adjunctions to Algebras", Bull. Amer. Math. Soc. 38 (1932) 85-88.

[FUCH 60] L. Fuchs, Abelian Groups, (Pergamon Press, Oxford, 1960).

[FUCH 68] L. Fuchs and I. Halperin, "On Embedding a Regular Ring in a Regular Ring with Identity", Fund. Math. 54 (1964), 285-290.

[FUCH 93] L. Fuchs, Infinite Abelian Groups, Vol. 2, (Academic Press, New York, 1993).

[FUNA 66] N. Funayama, "Imbedding a Regular Ring in a Regular Ring with Identity", Nagoya Math. J. 27 (1966), 61-64.

[GOOD 79] K.R. Goodearl, Von Neumann Regular Rings, (Pitman, London, 1979).

[MACL 71] S. MacLane, Categories for the Working Mathematician, (Springer-Verlag, New York, 1971).

[MCCO 86] N. McConnell, Embedding a Ring in a Ring with Identity, University of Tasmania, 1986.

[MCCO 87] J. C. McConnell and J. C. Robson, Non-Commutative Noetherian Rings, (John Wiley and Sons, New York, 1987).

[ROBS 79] J.C. Robson, "A Unified Approach to Unity", Comm. Algebra 7 (1979), 1245-1255.

[SILV 67] L. Silver, "Non-Commutative Localizations and Applications", J. Algebra 7 (1967) 44-76.

[STEN 75] B. Stenstrom, Rings of Quotients, (Springer- Verlag, New York, 1975).

[STOR 68] H.H. Storrer, "Epimorphismen von Kommutativen Ringen", Comment Math. Helv. 43 (1968) 378-401.

[STOR 73] H. H. Storrer, "Epimorphic Extensions of Non-Commutative Rings", Comment Math. Helv. 48 (1973), 72-86.

[VRAB 70] J. Vrabec, "Adjoining a Unit to a Biregular Ring", Math. Ann. 188 (1970), 219-226.