Embedding a Ring Into a Ring with Identity

Richard F. Maruszewski Jr.

Follow this and additional works at: https://epublications.marquette.edu/essays

Part of the Mathematics Commons
EMBEDDING A RING INTO A RING WITH IDENTITY

A Mathematical Essay

Presented to the mathematics department of Marquette University as a partial requirement for a Master of Science Degree

by

Richard F. Maruszewski, Jr.

June, 1966
The presentation of this paper is divided into three sections. The first of these sections is composed of proofs of different ways of embedding rings into rings with identity. The material in this section, which constitutes pages 1-10, is quite different from the material in the last two sections. Because of this difference, I followed a different method of presentation in the first section. The method used is to present a lecture outline, that is to produce the material just as I would in class. The last two sections are presented in a more narrative fashion. In section two, pages 10-14, we discuss applications of such embeddings. And the last section, pages 14-37, is concerned with finding all the rings with identity containing a given ring.
EMBEDDING A RING INTO A RING WITH IDENTITY

The purpose of this paper is to investigate the process of embedding a ring into a ring with identity. We first will show some different ways of embedding any ring into a ring with identity. We will then show some uses of such an embedding. Finally, we will investigate for a given ring all possible rings with identity which either contain the ring itself or an isomorph of it.

The following discussion on embedding a ring comes from Jacobson. We will follow the general outline of his proof.

Let $R$ be a ring. Let $B = I \times R = \{(m,a) | m \in I, r \in R\}$.

Let $(m,a) = (n,b)$ iff $m = n$, $a = b$.

Define $+$ by $(m,a) + (n,b) = (m+n, a+b)$.

$B$ is a commutative group.

a) Obviously $+$ is closed since $m+n \in I$, $a-b \in R$.

b) $(m,a) + (0,0) = (0,0) + (m,a) = (m,a)$.

c) $+$ is commutative and associative since the laws hold in $I$ and $R$.

d) $-(m,a) = (-m, -a)$. 
Define \( \cdot \) by \((m, a)(n, b) = (mn, na + mb + ab)\).

a) \[ [(m, a)(n, b)](g, c) = [(mn)g, g(na) + g(mb) + g(ab) + (mn)c + (na)c + (mb)c + (ab)c]. \]

b) \((m, a)[(n, b) + (g, c)] = (m, a)(n + g, b + c) = \]
\[ [(m(n + g), m(b + c) + (n + g)a + a(b + c)] = \]
\[ (mn + mb, mb + mc + na + ga + ab + ac). \]

By properties of multiples and associative laws in \( I \) and \( R \), the two are equal and therefore \( B \) is associative with respect to \( \cdot \).

b) \((m, a)[(n, b) + (g, c)] = (m, a)(n + g, b + c) = \]
\[ [(mn, na + mb + ab] \neq \]
\[ [mg, ga + mc + ac]. \]

A similar proof holds for the other distributive law.

Therefore \( B \) is a ring.

c) Consider \((1, 0) \in B, 1 \in I, 0 \in R.\)

\((1, 0)(m, a) = (m, a)(1, 0) = (m, a).\)

Therefore \( B \) is a ring with identity.

d) Consider \( R' \subseteq B = \{(0, a) | a \in R\}. \)

\((0, a) - (0, b) = (0, a - b) \in R'; \)
\((0, a)(0, b) = (0, ab) \in R'. \)

Therefore \( R' \) is a subring of \( B \).
e) Consider $\emptyset$ such that $a \in R$, $a\emptyset = a' = (0,a) \in R'$. Obviously $\emptyset$ is onto and 1-1.

$-(a+b)\emptyset = (0,a+b) = (0,a) + (0,b) = a\emptyset + b\emptyset$. 

$-(ab)\emptyset = (0,ab) = (0,a)(0,b) = a\emptyset b\emptyset$. 

Therefore $R \cong R'$ and is embedded in $B$, a ring with identity.

f) Also note $I' = \{(m,0)\}$. $I \cong I'$. 

$B = I' \cup R'$ or by the isomorphisms $I \cup R$.

g) $R'$ is an ideal in $B$, since 

$(m,a)(0,b) = (0,mb + ab) \in R'$ and 

$(0,b)(m,a) = (0,mb + ba) \in R'$.

h) Deficiencies in this method are:

1) If $R$ is a ring with an identity $e$, $z = (1,-e)$ is such that $za = 0$ for all $a$. $(1,-e)(0,a) = (0,-a + a) = (0,0)$. Thus if $R$ is a ring with identity we do not use this method.

2) The characteristic of $B$ may be different from that of $R$, for if the characteristic of $R = m \neq 0$, $B \not\cong I$; therefore the characteristic of $B \neq 0$.

3) If $R$ is an integral domain, $B$ may not be. 

Example: $R = \text{even integers}$ 

$(2,-2),(0,2m) \in B \neq 0$. 

$(2,-2),(0,2m) = (0,4m-4m) = (0,0)$. 

I will now proceed by presenting solutions to the last two deficiencies.

2) Let $R$ be a ring such that the characteristic of $R = m \neq 0$.

Let $G = \{ (\overline{n}, a) | \overline{n} = n + (m) \in I/\overline{m}, \ a \in R \}$.

Let $G = I/(m) \times R$.

a) Define addition by

\[ (\overline{n}, a) + (\overline{g}, b) = [(\overline{n} + \overline{g}), (a + b)] = (\overline{n + g}, a + b). \]

Define multiplication by

\[ (\overline{n}, a)(\overline{g}, b) = (\overline{ng}, nb + ga + ab). \]

Define equality by

\[ (\overline{n}, a) = (\overline{g}, b) \text{ iff } a = b, \ n = g. \]

b) Multiplication is single valued (well defined).

If $(\overline{n}, a) = (\overline{n'}, a')$ and $(\overline{g}, b) = (\overline{g'}, b')$,

\[ (\overline{n}, a)(\overline{g}, b) = (\overline{ng}, nb + ga + ab) \text{ and } \]

\[ (\overline{n'}, a')(\overline{g'}, b') = (\overline{n'g'}, n'b' + g'a' + a'b'). \]

But $g = g'$, $n = n'$, $a = a'$, $b = b'$ by definition of equality, therefore the operation is well defined.

c) $G$ is a ring with identity.

a) $(\overline{0}, 0)$ is the identity.

b) closed since $\overline{n} + \overline{g} = \overline{n + g}$

c) $-(\overline{n}, a) = (\overline{-n}, -a)$. 
d) $S$ is associative and commutative since the laws hold in $I$ and $R$.

- a) $S$ is associative as in the previous proof.
- b) $S$ is distributive as in the previous proof.
- c) $(1,0)$ is identity.

d) $R \cong G$. Define $\phi$ such that $a \mapsto (0,a)$.

1) Obviously $\phi$ is 1-1 and onto.
2) $(a+b)\phi = (0,a+b) = (0,a)+(0,b) = a\phi + b\phi$
3) $(ab)\phi = (0,ab) = (0,a)(0,b) = a\phi \circ b\phi$

e) Let $(\bar{n},a) \in G$;

\[ m(\bar{n},a) = (\bar{m},ma) = (\bar{m},ma) \neq (\bar{m},0) \]
since $R$ has a characteristic of $m$
\[ = (0,0) \] since $mn \in \langle m \rangle$.

Therefore we have embedded $R$ of characteristic $m$
into a ring with identity of the same characteristic.

3) Let $R$ be an integral domain.

Lemma 1 If $a, b \in R$, $a, b \neq 0$, $m \in I$ and such that

\[ ab + mb = 0, \]

then

- a) $ca + mc = 0$ for all $c \in R$.
- b) $ac + mc = 0$ for all $c \in R$.

Proof a) $(ca+mc)b = (ca)b+(mc)b$ distributive law in $R$
\[ = c(ab)+c(mb) \] properties of multiples
\[ = c(ab+mb) \] distributive law
\[ = c \cdot 0 \]
\[ = 0 \]
Since \( b \neq 0 \), \( ca - mc = 0 \), because \( R \) is an integral domain.

b) Assume \( ac + mc \neq 0 \).

If \( c \neq 0 \), obviously \( ac + mc = 0 \) and we have a contradiction.

If \( c \neq 0 \)

\[
\begin{align*}
&c(ac + mc) \neq 0 \\
&c(ac) + c(mc) \neq 0 \\
&(ca)c + (mc)c \neq 0 \\
&(ca + mc)c \neq 0
\end{align*}
\]

by part (a), \( ca + mc = 0 \)

\[\Rightarrow Oc = 0 \neq 0 \]

contradiction

Therefore \( ac + mc = 0 \) for all \( c \in R \).

1) Let \( B = (I \times R), -R = \) the integral domain above.

Let \( S = \{(m, r) \mid (m, r)(0, a) = (0, 0) \} \) for all \((0, a) \in R' \). 

We have shown \( R \cong R' \). Thus \( R \) is embedded in \( B \).

\[ S = \{(m, r) \mid (m0, r0 + ma + ra) = (0, 0) \} \] which is

\[ \{(m, r) \text{ such that } ma + ra = 0 \text{ for all } a \in R \} \]

\( S = \{(m, r) \mid ma + ar = ma + ra = 0 \} \) by preceding lemma.

ii) \( S \) is an ideal in \( B \).

a) If \((m, r), (m', r') \in S, (0, a) \in R' \)

\[
[m, r] - (m', r') \quad (0, a) = (m, r)(0, a) - (m', r')(0, a)
\]

\[= 0 - 0 = 0.\]
Therefore \((m,r)-(m',r') \in S\), implying 
\[ S \text{ is closed with respect to } +. \]

b) If \((m,r) \in S\), \((n,r') \in B\), then

\[(n,r')(m,r) = (nm, nr+mr'+r'r).\]

Let \((0,b) \in R'\). Then

\[(nm, nr+mr'+r'r')(0,b) = (0, nmb+nrb+mr'+rr'b).\]

Therefore \((n,r')(m,r) \in S\). Since

\[(m,r)(n,r') = (mn, mr'+nr+rr'),\]

\[(mn, mr'+nr+rr')(0,b) = (0, mnb+mr'b+nrb+rr'b) = (0, n0+Ob) = (0,0).\]

Therefore \((n,r')(m,r) \in S\). Since

\[(m,r)(n,r') = (mn, mr'+nr+rr'),\]

\[(mn, mr'+nr+rr')(0,b) = (0, mnb+mr'b+nrb+rr'b) = (0, n0+Ob) = (0,0).\]

Thus \(S\) is an ideal in \(B\).

iii) It follows that \(B/S\) is a ring with identity of form:

a) \(B/S = \{(n,r') \uparrow S \mid (n,r') \in B\}\)

b) The identity is \((1,0) \uparrow S\).
iv) B/S is an integral domain.

a) Assume \[ (m, r) + S, (n, r') + S \in B/S \]
such that they are non-zero,
that is \( (m, r), (n, r') \notin S \).

b) Therefore \( (m, r)(0, a)(0, a) \neq (0, 0) \) and
\( (n, r')(0, a)(0, a) \neq (0, 0) \)
for any \( a \in R \) since otherwise by our lemma this would imply they are
elements of \( S \).

c) Assume \[ (m, r) + S, (n, r') + S \]
This implies \( (m, r)(n, r') \in S \),
that is \[ (m, r)(n, r')(0, a) = (0, 0) \].
Therefore \( (m, r)[(n, r')(0, a)] = (0, 0) \)
by the associative law.

Therefore \( (m, r)(0, na + r'a) = (0, 0) \),
but note the second term \( R' \Rightarrow \)
\[ m(na + r'a) + r(na + r'a) = 0 \Rightarrow \]
\( (m, r) \in S \) by our lemma.

But this contradicts our original assumption.
Therefore \( (m, r)(n, r') \notin S \)
\[ \Rightarrow (m, r) + S, (n, r') + S \notin 0, \text{ which implies } \]
\[ B/S \text{ is an integral domain.} \]
v) Let \( \tilde{S} = \{(0,a) + S | (0,a) \in R^2 \} \).

a) \( \tilde{S} \) is a subring of \( B/S \).

1) Let \((0,a) + S; (0,b) + S \in \tilde{S}; a,b \neq 0\).

\[
[(0,a) + S] - [(0,b) + S] = (0,a-b) + S \in \tilde{S}.
\]

2) \[
[(0,a) + S] \cdot [(0,b) + S] = (0,ab) + S \in \tilde{S}.
\]

Therefore \( \tilde{S} \) is a subring of \( B/S \).

b) \( R \cong S \). Define \( \emptyset \) such that \( a\emptyset = (0,a) + S \),

\[ R \to \tilde{S}. \]

1) \( \emptyset \) is obviously onto.

2) If \((0,a) + S = (0,b) + S\),

\[
(0,a) = (0,b) + (m,r) \text{ such that } (m,r) \in S
\]

\[
= (0+m, b+r) \text{ implying } m = 0.
\]

Therefore \((0,a) = (0,b) + (0,r)\)

such that \((0,r) \in S\).

Since \((0,r) \in S\), \((0,r)(0,a) = (0,0)\)

and \( ra = 0 \).

Similarly \((r,b) = 0\). Since \( a,b \neq 0\),

\( r = 0 \) for \( R \) is an integral domain.

Therefore \((0,a) = (0,b)\)

impllying \( a = b \) and

\( \emptyset \) is 1-1.
3) \((a+b)\mathbb{0} = (0,a+b) + S = [(0,a) + S] \\
+ [(0,b) + S] = a\mathbb{0} + b\mathbb{0}\)

\[(ab)\mathbb{0} = (0,ab) + S = [(0,a) + S] [(0,b) + S] \\
= a\mathbb{0}b\mathbb{0}\]

Therefore \(\mathbb{0}\) is an isomorphism and \(R \cong S\), and therefore \(R\) is embedded in \(B/S\), an integral domain.

Thus, we may embed any ring into a ring with identity. In fact certain special rings such as a ring with a given characteristic or an integral domain can be embedded into a ring of the same type.

It might now be interesting to look at some uses of the embedding theorem. I will consider only two uses here, but it is well to remember that these are but two of many uses our theorem has in the development of ring theory.

In discussion of Polynomial Rings, it can be shown that if we have a ring with identity, we can form \(R[x]\) such that \(x\) is transcendental, that is

\[a_1x_1 = 0 \text{ iff } a_1 = 0, \ 1 \leq 1, 2, \ldots, n.\]

Following from this theorem are various other results which hold for transcendental polynomial rings. Thus if our ring does not have an identity we cannot continue.
But if we can embed our ring into a ring with identity:

\[ R \to R' \leq R^* , \]

\( R^* \) a ring with identity and \( R' \) a subring of \( R^* \);
we can identify \( R \) with \( R' \) and thus consider \( R[x] \) a subring of \( R^*[x] \).

Also once we have embedded our ring into a ring with identity, we can construct a ring with identity containing our ring by the following method.

Let \( T = R \cup ([I \times R] \cdot R') \).

\[ T = \{ r \text{ or } (m,r') | m \in I; r,r' \in R \text{ if } m \neq 0 \}. \]

Define \( \eta : I \times R \to T, \)

\[ (0,a) \mapsto a, \]

\[ (m,r) \mapsto (m,r), m \neq 0. \]

Since \( R \cong R' \), it is obvious that \( \eta \) is one to one and onto.

Therefore, it is possible to turn \( T \) into a ring isomorphic to \( I \times R \).

**Proof:**

1) Define \( + \) such that \( \eta(t_1, t_2) \to T \) for all

\[ \eta(y_1, y_2) \in I \times R \text{ such that } \eta(y_1) = t_1, \eta(y_2) = t_2. \]

\[ t_1 + t_2 = \eta(y_1 + y_2) = (y_1 + y_2). \]

Thus \( (m,r) + (n,r') = (m+n,r+r') \), \( m,n \neq 0 \),

and \( r + (m,r') = (m,r+r') \).

a) Obviously \( + \) is closed by above.

b) \( 0 \) is identity.

\[ a + 0 = (0,a) \eta \to (0,0) \eta = (0,a) \eta = a \]

(continued...)
\[(m,r) + 0 = (m,r) \eta + (0,0) \eta = [ (m,r) + (0,0) ] \eta = (m,r) \eta = (m,r).\]

c) \(a \in \mathbb{R}\) has an inverse \(-a\).
\[a + -a = (0,a) \eta + (0,-a) \eta = (0,0) \eta = 0.\]
\[(m,r)\) has inverse \((-m,-r)\).

d) Obviously \(+\) is commutative and associative since these laws hold in \(I\) and \(\mathbb{R}\).
\[a + r = (0,a) \eta + (0,r) \eta = (0,a+r) \eta = (0,r-a) \eta = r+a\]
\[(m,r) + (n,r) = (n,r) + (m,r)\) etc.
Therefore \(T\) is a group under \(+\) defined.

i) Define \(\cdot\) by \(t_1 \cdot t_2 = \gamma_1 \eta \gamma_2 \eta = \gamma_1 \gamma_2 \eta\).

a) Obviously \(\cdot\) is closed.
\[r_1(r_2) = [(0,r_1)(0,r_2)] \eta = (0,r_1 r_2) \eta = r_1 r_2\]
\[(m,r)(n,r') = (m,r)(n,r') \eta = (mn, nr + mr' + rr') \eta\]
\[(mn, nr + mr' + rr') \eta\]
\[(m,r) r_1 = (m,r) \eta (0,r_1) \eta = [(m,r)(0,r_1)] \eta = (0, mr_1 + rr_1) \eta = mr_1 + rr_1\]

b) \(T\) is associative. \((rr_1)(r_2) = (r)(r_1 r_2)\)
\[[m,r](n,r') (g,r'') = (m,r) \[(n,r')(g,r'')\]
\[[r_1(m,r)](n,r') = [(0,r_1) \eta (m,r) \eta] (n,r') \eta = [0, mr_1 + rr_1] (n,r') \eta = [nmr_1 + nr_1 + mr_1 r'' + r_1 rr'']\]
\[
\begin{align*}
\text{d) Consider } (1,0) \in T. \text{ Since } 1 \neq 0, \\
& a(1,0) = (0,a)(1,0) = \{0,a\}(1,0) \\
& = (0,a) = a \\
& (m,r)(1,0) = (m,r)(1,0) = \{m,r\}(1,0) \\
& = (m,r) = (m,r)
\end{align*}
\]

Therefore \( T \) is a ring with identity, 

\((1,0)\) containing \( R \).

Let \( \bar{T} = \{ (t_1,t_2,\ldots,t_n,0,0,\ldots) \mid t_i \in T, \text{ all but a finite number are zero} \} \)

\(\bar{T}\) under \( + \) is a group.

\begin{enumerate}
  \item \( + \) is commutative and associative in \( \bar{T} \)
    since \( + \) is in \( T \).
  \item The inverses are \((-t_1,-t_2,\ldots,-t_n,0,0,\ldots)\).
  \item The identity is \((0,0,\ldots,0)\).
\end{enumerate}

They hold in \( T \).

\(((1,0),0,0,\ldots)\) is identity.

b) Consider \( T' = \{ t,0,0,0,0,\ldots \} \), \( t \in T \).

\( T' \) is a subring of \( \bar{T} \) such that \( T \cong T' \).

c) Let \( x = (0,(1,0),0,0,\ldots) \).
\[ x^2 = (0,0,(1,0),0,0\cdots) \]
\[ x^3 = (0,0,0,(1,0),0\cdots) \]

etc.

Consider \( (a_0,a_1,\cdots,a_n,0,\cdots) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \).

In fact \( \overline{T} = T[x] \) such that \( x \) is transcendental.

Another important theorem in ring theory is Cayley's theorem for rings, which states that any ring with identity is isomorphic to a ring of endomorphisms. Again if \( R \) does not have a unity the theorem does not hold. But as in the preceding discussion we can embed our ring into a ring with identity and continue.

Or as in the preceding discussion, once we have embedded \( R \) in \( I \times R \) or in general have embedded it in a ring with identity, we can construct a ring with identity containing \( R \). If we again call this ring \( T \), we can show \( R \) is isomorphic to a ring of endomorphisms which is a subring of \( \text{Hom}(T,T) \).

It is now of interest to investigate the set of all rings with identity containing a given ring. Our discussion will closely follow the outline set down by Brown and McCoy\(^2\).

Definition: Let \( R \) be our ring and let \( G \) and \( T \) be rings containing \( R \), an isomorphism of \( G \) onto \( G' \), a subring of \( T \), is called strict iff each element of \( R \) is self-corresponding.

\[ R \trianglelefteq G \trianglelefteq G' \trianglelefteq T \]
Definition: Let \( R \) be contained in a given set \( D \) of rings. A subset \( S \) of \( D \) is called a **complete set of extensions** of \( R \) in \( D \) iff

1. each ring \( G \) in \( S \) is a ring with unit containing \( R \).
2. if \( T \) is a ring in \( D \) with a unit, then there are rings \( G \) and \( G' \) in \( S \) such that \( G \cong G' \leq T \).

Definition: \( S \) is said to be a **minimal set of extensions** of \( R \) in \( D \) iff \( S \) is complete in \( D \) and no proper subset of \( S \) is complete in \( D \).

Definition: If the complete set of extensions \( S \) consists of only one ring \( G \), we refer to \( G \) as a **minimal extension** of \( R \) in \( D \).

We thus are interested in looking at all the rings with unit containing our ring \( R \). We would like to find all the members of \( D \), the minimal set \( S \), and the conditions that \( R \) have a minimal extension in \( D \).

We can also break our study of \( D \) into two cases:

1. finding all the members of \( D \) and
2. finding the subset of \( D \) whose rings have the same characteristic as \( R \).

First, we must define certain properties and ideas which will be of extreme importance in our theory later.

If \( G \) is one of our rings containing \( R \), it is possible
that there exist certain integers m such that me \leq R even though R does not contain a unit itself. Moreover if me \leq R,

(me)r = r(me) = mr for all r \in R, that is

if a \in R such that a = me, e \in G, m \leq I,

(l) \ar = ra = mr for all r \in R.

Definition: The set of all integers m such that (l) is true for some a \in R is an ideal in the ring of integers and the generator of this ideal is the mode of R.

Proof: a) Let m, n \in the set,

there exists a \in R such that ar = ra = mr, r \in R and there exists b \in R such that

br = rb = nr.

(m - n)r = mr - nr = ra - rb = r(a - b)

= ar - br = (a - b)r.

b) Let m \in the set, g \in I,

then ar = ra = mr for some a \in R and

(gm)r = g(mr) = gra = g(ar)

= m(gr) = (gr)a = a(gr).

Similarly for the left side, the proof follows implying we have an ideal.

Note: If R has a unit, its mode is 1.

For r \in R and m \leq I, ar = ra = mr for all r \in R

a = ml \in R since 1 does.

Note: Mode turns into a fundamental concept later on.
Let $R$ be a ring, $a \in R$, $m \in I$, such that $ra = ar = mr$, that is $a = me$ for $r \in R$.

Definition: $a$ is said to be an $m$-fier of $R$, and $m$ is said to have an $m$-fier of $a$ in $R$.

Thus $0 \in R$ is a zero-fier of $R$ since $0 = Oe = Oa = aO = Oe$ for all $a \in R$. The integer zero is said to have a 0-fier over the zero $\in R$. If $R$ has a unit $e$, $e$ is the unique 1-fier of $R$.

Proof: $e = le$. $re = er = r = 1r$. The uniqueness of $e$ gives fact that 1-fier is unique.

Lemma: The set of all integers $m$ which have $m$-fiers of $R$ is an ideal $K$ in $I$.

---proven earlier.

Lemma: The set of $m$-fiers is a subring of $R$ called $M$.

Proof: Let $a, b$ be such that $ra = af = mr$, $a = me$.

\begin{align*}
rb &= br = nr, & b &= ne.
\end{align*}

1. $(a-b)r &= ar - br &= ra - rb = r(a-b) \\
&= (me-ne)r = (m-n)r
\end{align*}

2. $abr &= arb = rab = mener = mrn.

Thus $M$ is a subring.
Definition: The ideal $K$ may be called the modal ideal of $R$. Since $K \subseteq I$, $K = \{m\}$ such that $m$ is called the mode of $R$.

$$K = \{m | m \in I, m \in R\}$$

Definition: An element of $M$ is called a modifier of $R$.

$$M = \{a | a \in R, a = me \text{ for some } m \in I\}$$

Lemma--Definition: The subset of $K$ such that $mr = 0$ for all $r \in R$ is an ideal $N$ in $I$ and therefore in $K$.

Proof: Let $g, p \in N$ then

$$gr = rg = 0 \quad r \in R.$$  
$$pr = rp = 0 \quad r \in R.$$  
$$(g - p)r = r(g - p) = 0$$  
$$m(p)r = p(m)r = 0$$

Lemma--Definition: The corresponding subset of $M$ called $P$ is a two sided ideal in $R$ and therefore in $M$.

Proof: $P = \{a \in R | ar = ra = 0, r \in R\}$

$$(a - b)r = 0 = r(a - b).$$  
$$car = acr = 0.$$  

Definition: $N$ is said to be the characteristic ideal of $R$ and since $N \subseteq I$, $N = \{v\}$, $v \in I$, $v$ called the characteristic of $R$.

Definition: An element of $p$, that is a $c \in R$ such that $ar = ra = 0$ for all $r \in R$ is called an annihilator of $R$. 
Note: If more than one ring is under discussion, ideals in I, generators, etc. are associated with their ring by subscript, that is the characteristic ideal of ring $T$ is $N_T$ with generator $v_T$.

Immediate Consequences

A) The characteristic is a multiple of the mode.

Proof: The mode is the generator of $K$; the characteristic is the generator of $N$; but $N$ is an ideal in $K$; by Lagrange's theorem

$$v/m = m = pv.$$

B) If $a$ is a m-fier and $l \in P$, $g \in N$, then $a + l$ is a $(m+g)$-fier.

Proof: $(a + l)r = ar + lr = ar + 0 = ra + rl = r(a + l) = mr + gr = (m+g)r$.

In particular $0 \in R$ is a v-fier, $vr = 0$.

C) If $a, b$ are m-fiers then $a-b \in P$ that is

$$ar = ra = mr = br = rb$$

$$(b-a)r = br-ar = mr-mr = 0.$$ Therefore if $P = (0)$, $a, b$ being m-fiers means

$$a-b = 0, a = b$$

and

therefore the m-fiers are unique.

D) If $R$ and $T$ are rings $R \leq T$, $N_R \supseteq N_T$ by the obvious proof.
**Theorem 1:** Let $R$ be a ring, $M/P \cong K/N$.

**Proof:** Let $a'$ denote the coset in $M/P$ which contains the element $a$ of $M$.

Let $m'$ be the coset in $K/N$ containing $m$ in $K$.

Define $\phi: a' \rightarrow m'$ iff $a$ is an $m$-fier of $R$.

**Note:** If $a' \rightarrow m'$ and $a_1' \rightarrow m_1'$,

\[(a_1-a)r = r(a_1-a) = (m_1-m)r\]

If $a_1' = a'$, $a_1-a \in P$, and $(m_1-m)r = 0$. Therefore $m_1-m \in N$

and $m_1' = m'$.

Thus $\phi$ is well defined.

If $m_1' = m'$, $m_1-m \in N$,

\[(a_1-a)r \in r(a_1-a) = 0, \text{ implying } (a_1-a) \in P \text{ and } a_1' = a'.\]

Therefore $\phi$ is 1-1.

Obviously $\phi$ preserves sums and products.

**Examples:**

1) $(u)$ in $I$ It is obvious that the mode is $u$.

The characteristic $\nu = 0$.

2) $(0)$ in $I$ $(0)$ is the only one element ring.

The mode 1. The characteristic is obviously 1. In fact any ring of prime characteristic has mode equal to characteristic.
3) A ring with unit. The generator of \( K \) is \( k = 1 \).
\( P = \langle 0 \rangle \).

4) A ring with characteristic \( v \) such that every product is zero.
\[ M = P = R \]
\[ R \text{ has } k = v, \text{ that is } K = N \text{ since } K/N \cong P/M \]

5) \( R \) a subring of \( I/(24) \) consisting of
\[ \bar{0} \ 4 \ 8 \ 12 \ 16 \ 20. \]
\[ M = R \text{ since every member of } R \text{ can be expressed as an integer times } 1. \]
\[ P = \{ \bar{0}, \bar{12} \}. \]

The mode is 2. The characteristic is 6.

**Definition:** Now consider \( a \), a fixed element of \( R \). The set of integers \( u \in I \) such that \( ua = 0 \) is an ideal, denoted by \( H_a \) in \( I \).

**Proof:** Let \( H_a = \{ u \in I | ua = 0 \} \)

Let \( u_1 \) and \( u_2 \in H_a \)

1) \( (u_1 - u_2)a = u_1a - u_2a = 0; \)
   therefore \( u_1 - u_2 \in H_a \)

2) Let \( m \in I, \ u \in H_a \),
   \[ (mu)a = m(ua) = 0 \]
   \[ (um)a = m(ua) = 0. \text{ Thus } H_a \text{ is an ideal.} \]

**Definition:** The ideal \( H_a \) is called the order ideal of \( a \).

**Definition:** The generator of \( H_a \), denoted by \( n_a \), is called
the order of $a$.

**Note:** $0 \in R$ is the only ideal of order 1, that is for all $m \in I$, $m0 = 0$; if $a \in R$ such that $ma = 0$ for all integers $\rightarrow la = 0 \rightarrow a = 0$.

**Note:** If $R$ had a unit $e$, $ne = v$ since the characteristic of $R$ is the least positive integer which takes $e$ to zero.

**Lemma:** Clearly $N = \bigcap_{r \in R} H_r$ for all $r \in R$.

**Lemma:** Since $H_r \supseteq N$, for all $r$, it follows that $n_r / v$.

**Lemma:** $n_{-a} = n_a$.

The following results become evident:

E) The order $n_{a \pm b}$ of $a \pm b$ is the least common multiple of $n_a$ and $n_b$.

F) If $(n_a, n_b) = 1$, $n_{a \pm b} = n_a n_b$.

G) If $\theta \in I$, the order ideal of $\theta a$ is the ideal quotient $H_a : \theta = \{ \lambda \in I | \lambda \theta \in H_a \}$.

Or in terms of generators, $n_{\theta a} = n_a / (n_a, \theta)$

if $(n_a, \theta) \neq 0$;

$n_{\theta a} = 1$ if $(n_a, \theta) = 0$.

H) If $a$ is an m-fier, that is $a = me$, $H_a \subseteq N : m$.

and if $P = (0)$ then $H_a = N : m$.

**Proof:** If $u \in H_a$, then $ua = 0$. Therefore since $a$ is an m-fier, $ume = 0$. Therefore $umr = 0$ for
all \( r \in R \). Therefore \( um \in N \). Therefore \( u \in N : m \).

If \( P = \{0\} \) and \( u \in N : m \), then \( um \in N \).

Therefore \( (ua)r = r(ua) = 0 \) for all \( r \in R \).

Hence \( ua \in P \). Therefore \( ua = 0 \). Therefore \( u \in H_a \).

I) The order of an annihilator is a divisor of the mode.

Proof: Let \( m \in K \) and let \( a \) be a \( m \)-fier. If \( l \in P \)
then by B) \( a + l \) is an \( m \)-fier. Then it follows

from A) that \( ml = 0 \rightarrow m \in H_1 \). Therefore

\( K \subset H_1 \) for all \( l \), and I) follows immediately.

J) If \( a \) and \( b \) are \( m \)-fiers of the same order \( n \) and

\( (n,k) = 1 \), then \( a = b \).

Proof: Since \( a \) and \( b \) are \( m \)-fiers, \( a - b \in P \)

following from \( \emptyset \).

Hence \( n a - b \in K \) by I), but \( (n,k) = 1 \).

Therefore \( n_{a-b} = 1 \). Therefore \( a - b = 0 \).

Therefore \( a = b \).

We now will try to find the complete set of extensions of

a given ring \( R \).

Let \( U \) be the set of ordered pairs \([r,u] \) such that \( r \in R \)

\( u \in I \) such that a) equality defined in usual way

b) \([r_1,u_1] + [r_2,u_2] = [r_1 + r_2,u_1 + u_2]\)

c) \([r_1,u_1] \cdot [r_2,u_2] = [r_1 r_2 + u_1 r_2 + u_2 r_1, u_1 u_2]\)

Note: This is similar to our original manner of embedding.
Obviously from our preceding discussions $U$ is a ring with unit $[0,1]$ and $\{[r,0]\}$ is a subring of $U$ isomorphic to $R$.

In $U$ the set of integral multiples of the element $[-a,m]$, $a$ being an $m$-fier of $R$ is a two sided ideal denoted by $g(a,m)$.

Denote $U/g(a,m)$ by $R(a,m)$, which is defined iff $a$ is an $m$-fier and $m \neq 0 \Rightarrow a = 0$.

The coset of $g(a,m)$ in $R(a,m)$ which contains $[r,u]$ of $U$ will be denoted by $(r,u)$. Thus in $R(a,m)$, $(r_1,u_1) = (r,u)$ iff $[r_1,u_1] - [r,u] \in g(a,m)$; that is iff for some integer $\lambda$,

$\begin{align*}
(1) \quad & r_1 - r = -\lambda a \quad \text{and} \quad u_1 - u = \lambda m.
\end{align*}$

It is clear that $R(0,0) \cong U$ and that each $R(a,m)$ has a unit since $U$ does and is commutative iff $R$ is.

In $R(a,m)$, $(r,u) = (r-\lambda a, u+\lambda m)$, following from the discussion above.

In particular, $(r+\lambda a,u) = (r,u+\lambda m)$. Also it is obvious that $R(-a,-m) = R(a,m)$. Therefore we can restrict ourselves without loss of generality to $m \geq 0$.

Consequent Results

K) The characteristic of $R(a,m)$ is $m \cap a$

Proof: The characteristic of $R(a,m)$ is the order of its unit $(0,1)$ by theorem. Now if $B \in H(0,1)$, then $B(0,1) = (0,B) = (0,0)$. 
Therefore by (1) there is some \( \lambda \) such that
\[
0 = -\lambda a, \quad B = \lambda m \rightarrow \lambda e(ra), \quad B \in (mn_a).
\]
Conversely if \( B \in (mn_a) \) then \( B = \sigma_{mn_a} \) and
\[
0 = -\sigma_{mn_a} \text{ so } (0, B) = (0, 0) \text{ by (1) and } B \in H(0,1).
\]
Hence \( H(0,1) = mn_a \).

L) The correspondence \( r \mapsto (r, 0) \) is an isomorphism of
\( R \) onto a subring of \( R(a, m) \).

a) Obviously \( \phi \) preserves sums and products.

b) Also obviously \( \phi \) is onto.

c) Suppose \( (r_1, 0) = (r, 0) \), then \( r_1 - r = -\lambda a \) and
\[
o = \lambda m. \text{ But by (1) if } m \neq 0 \rightarrow \lambda = 0.
\]
Therefore \( r_1 - r = 0 \). Therefore \( r_1 = r \).

If \( m = 0 \) then by definition of \( R(a, m) \), \( a = 0. \)

Hence \( r_1 = r \). Therefore \( 1 \)-1.

Note: L) would not be true in general if we
had defined \( R(a, m) \) in the case \( a \neq 0 \)
and \( m = 0 \). That is why we excluded that case.

We now construct a ring containing \( R \) isomorphic to
\( R(a, m) \) in the usual manner:

Let \( R^*(a, m) \) be the ring whose elements consist of
\( R \) and the elements of \( R(a, m) \) of form \( (r, u) \) \( u \neq 0(m) \),
that is cannot be put in form \( (r, 0) \).

Let \( f \) denote the \( 1 \)-1 correspondence between \( R \)
and \( R^*(a, m) \) defined by \( r \mapsto (r, 0) \) and
\( (r, u) \mapsto (r, u), \ u \neq 0(m). \)
Define sum and products as the inverse image of the sums and products of the images of these elements under \( f \).

**M)** \( R^*(a,m) \) is a ring with unit containing \( R \) which is isomorphic to \( R(a,m) \) under \( f \).

We thus have a set of rings \( \{ R^*(a,m) \mid a \) is an \( m \)-fier of \( R, m \in \mathbb{J} \} \), each one of which has a unit and contains \( R \).

**Examples:**
6) If \( R \) has a unit \( e \), then \( R^*(e,1) \) is identical to \( R \) since \((r,u) = (r + ue, 0)\) in \( R(e,1) \).

7) If \( R \) is the null ring, \( R(0,m) \cong \mathbb{Z}/(m) \) under \((0,m) \rightarrow \bar{m}\).

8) If \( R \) is the ideal \((m)\) in \( I \), then \( R(m,m) \cong I \) by \((r,u) \rightarrow r + u\).

**N)** If a ring \( R \) is contained in a ring \( G \) with unit \( e \), then the set of integers \( u \) such that \( ue \in R \) is an ideal \( \mathcal{T}_G = (v_G), v_G \geq 0 \) in \( I \). \( N_G \leq \mathcal{T}_G \leq \mathbb{Z}_R \).

Note: If \( N_G = N_R \), then \( N_R \leq \mathcal{T}_G \leq \mathbb{Z}_R \), that is \( v_G \) is a divisor of the characteristic and a multiple of the mode.

**Theorem 2:** The set \( C = \{ R^*(a,m) \mid a \) is an \( m \)-fier of \( R \) and \( m \in \mathbb{J} \} \) is a complete set of extensions of \( R \) in the set of all rings. More specifically in the notation of \( N \), each member of \( C \) is a ring with unit which contains \( R \); and if \( G \) is a ring with identity \( e \)
which contains \( R \) then there are rings \( R^*(v, v) \) in \( G \) and \( G_1 \) such that

\( (ii) \ R^*(v, v) \cong G_1 \leq G \) where \( v = \sqrt{v} \).

**Proof:** Let \( G_1 \) be the set of elements of \( G \) of the form \( r + u e, \ r \in R, \ u \in I \). Consider the map \( R(v, v) \rightarrow G_1 \) defined by \( (r, u) \rightarrow r + u e \).

Clearly by (i) \( (r_1, u_1) = (r, u) \rightarrow r_1 + u_1 e = r + u e \). Therefore the map is well defined.

Furthermore if \( r_1 + u_1 e = r + u e \) then

\( (r_1, u_1) = (r, u) \) for \( (r_1 - r) = -(u_1 - u) e \rightarrow u_1 - u \in \sqrt{\Gamma} \); therefore \( u_1 - u = \lambda \sqrt{v} \); therefore \( r_1 - r = -\lambda v e \). So by (i)

\( (r_1, u_1) = (r, u) \). Therefore the map is 1-1.

Obviously the function preserves sums and products. Therefore it is an isomorphism, which we will denote by \( f_1 \).

Let \( f \) be the isomorphism of \( M \). Then

\( f_1 f \) is the required isomorphism of \( R^*(v, v) \) onto \( G_1 \).

Let \( \mathcal{A}_v \) denote the set of rings with characteristic \( v \).

Let \( \mathcal{C}_v \) denote the intersection of the sets \( \mathcal{C} \) and \( \mathcal{A}_v \). Then

**Corollary:** If \( R \in \mathcal{A}_v \), then \( \mathcal{C}_v \) is a complete set of extensions of \( R \) in \( \mathcal{A}_v \).
Proof: If $G$ has characteristic $v$, contains $R$, and has unit $e$ then for some $G_1$, $v = v_G$, $R \subset R^*(ve, v) \leq G_1 \leq G$ where $R^*(ve, v) \leq G_v$ and $G_1 \leq A_v$ since $H_R = H_G = (v)$.

C) There exists a homomorphism from $R^*(a, m)$ to $I/(m)$ with kernel $R$.

Proof: Let $\lambda$ denote the map from $R(a, m) \to I/(m)$ defined by $(r, u) \mapsto \bar{u}$.

Then $\lambda$ is a homomorphism since by (1) if $(r_1, u_1) = (r, u)$ then $u_1' = u'$; and sums and products are obviously preserved.

K elements $(r, u)$ such that $u' = 0'$ or $u = \lambda m$, namely all of form $(r, \lambda m) = (r + \lambda a, 0)$ or of form $(r, 0)$, $r \in R$.

If $f$ is again the isomorphism of $M)$ $\lambda f$ is the homomorphism required.

Lemma 1: If $R^*(b, \beta)$ contains a strict isomorph $\mathfrak{A}$ of $R^*(a, m)$ then $I/(\beta)$ contains an isomorph of $I/(m)$.

Proof: Since $R^*(a, m) \cong \mathfrak{A} \subset R^*(b, \beta)$ by $0$ we have $I/(m) \cong R^*(a, m)/R \cong \mathfrak{A}/R \subset R^*(b, \beta)$.

Theorem 3: A ring $R$ has a minimal extension $G$ in the set of all rings iff the mode of $R$ is $0$ or $1$.

Proof: Necessity By hypothesis, there is a set $S$ consisting of just one ring $G$ with unit $e$.
which contains \( R \) with the property that if \( F \) is a ring with unit which contains \( R \); there exists \( G' \) such that \( G \cong G' \subset F \).

We shall prove first that in the notation of \( N) \Gamma_G = K_R \). By \( N \) we need only that \( K_R \subset \Gamma_G \). For ring \( G \) there exists by Theorem 2 a ring \( G_1 \) such that (ii) holds with \( v = v_G \). Let \( K_R = (k), k \geq 0 \). Let \( k \) be a \( k \)-fier of \( R \). Since the ring \( R^*(k, k) \) has a unit and contains \( R \) there is by hypothesis a ring \( G' \) such that \( G \cong G' \subset R^*(k, k) \). Combining this with (ii), \( R^*(k, k) \) contains an isomorph of \( R^*(v_G, v) \). Hence by Lemma 1, \( I/(k) \) contains an isomorph of \( I/(v) \). It follows from D) that \( K_R \subset \Gamma_G \). Therefore \( \Gamma_G = K_R \).

Therefore \( v = k \).

Since \( R^*(0, 0) \) with unit contains \( R \), there is by hypothesis a ring \( G_0' \) such that \( G \cong G_0' \subset R^*(0, 0) \). Combining this with (ii) and Lemma 1, we have that \( I/(0) \) contains an isomorph of \( I/(v) \) which in turn implies \( v = 0 \) or \( v = 1 \). But \( v = k \), therefore, the mode must be zero or 1.

**Sufficiency** If the mode of \( R \) is 1, \( R \) must have unit; and therefore it is itself
the required ring $G$.

If $k = 0$ and $F$ is any ring with unit containing $R$, then by (ii) $\Gamma_F = (0)$.

Hence by Theorem 2, there is a ring $F_1$ such that $R^*(0,0) \cong F_1 \subseteq F$. Therefore, $G$ is $R^*(0,0)$.

**Corollary 1:** No ring of positive characteristic without a unit has a minimal extension in the set of all rings.

**Proof:** follows directly from Theorem 2.

**Example:** If $C =$ Complex Numbers, $R$ the ideal $(x)$ in $C[x]$, then $R$ is a ring of mode 0. Therefore, $R$ has a minimal extension in the set of all rings; namely $R^*(0,0)$, such that $R^*(0,0)$ is isomorphic to a subring of $C[x]$, consisting of all the polynomials with constant terms in $I$. Every ring with unit containing $R$ contains an isomorph to this ring.

P) If $\nu = 0$ and $I/(\nu)$ contains an isomorph of $I/(\delta)$ then $(\delta', \nu/\delta') = 1$.

**Lemma 2:** If $(m, \Theta) = 1$ then $R^*(\Theta a, \Theta m)$ contains a strict isomorph of $R^*(a, m)$. 
Proof: If \( \Theta = 0 \) then \( m = 1 \) and \( R \) has a 1-fier, \( a = e \).
Hence \( R^w(e,1) \sim R \leq R^w(0,0) \). If \( m = 0 \), the lemma is trivial. So suppose \( \Theta m > 0 \).
Then there exist integers \( p, n \) such that \( pm + n\Theta = 1 \). Detailed calculations yield
that \( (r,u) \mapsto (r \cdot up, un\Theta) \) defines a correspondence from \( R(a,m) \) into \( R(\Theta a, \Theta m) \)
which is in fact an isomorphism into (denoted by \( f_1 \)). If \( f \) is the isomorphism 
\( \Phi \circ M \) and \( f_\Theta \) the analogous isomorphism 
from \( R^w(\Theta a, \Theta m) \) onto \( R(\Theta a, \Theta m) \), then \( f_\Theta \circ f_1 \circ f \)
is our required isomorphism.

Theorem 4: If \( R \) is a ring of prime mode \( k \) with unique annihilator \( 0 \) then \( R \) has a denumerable minimal set of extensions in the set of all rings.
Proof: Since \( R \) has only one annihilator \( 0 \), 
every \( m \)-fier is unique by \( C \). Hence
if \( \kappa \) is the unique \( k \)-fier and \( R\kappa = 
R^w(\lambda \kappa, \lambda \kappa) ; \lambda = 0,1,2 \cdots \), then the
set \( A \) of Theorem 2 is just the set \( R\kappa \).
We shall prove that the denumerable subset \( S = R_0, R_1, R_\kappa, R_{\kappa^2}, \cdots \) of \( \{R\kappa\} \)
is minimal in the set of all rings.
1) To prove $S$ is complete. Since 
\[ \{R_{\lambda}\} \] is complete any ring $F$ with unit which contains $R$ contains a strict isomorph of some ring, say $R_{\sigma}$, in 
\[ \{R_{\lambda}\} \]. If $\sigma \not= 0$ then $R_0$ is the desired ring of $S$. If $\sigma > 0$ then 
$\lambda = uk^v$, $v \geq 0$, $(u,k) = 1$. Therefore by Lemma 2, the ring $R_{\lambda} = R_\sigma(uk^v, uk^{v+1})$ contains a strict isomorph $R_\sigma(k^v, k^{v+1}) = R_{kv}$ which is the desired ring in $S$.

11) Minimal. If some proper subset of $S$ is complete in the set of all rings then some ring of $S$ contains an isomorph of another ring of $S$. Hence by Lemma 1, one of the following must be true for $\alpha, \beta$ distinct integers

1) $I/(0)$ contains an isomorph of $I/(k^\alpha)$
2) $I/(k^\alpha)$ contains an isomorph of $I/(0)$
3) $I/(k^\alpha)$ contains an isomorph of $I/(k^\beta)$

But all three of these are impossible. (2) by P) Therefore $S$ is minimal.

Example: 9: Consider the ring $B$ of polynomials in the indeterminate $x$ with integral coefficients and even constant terms.
Let R be the ring $B/(x^2-2)$. The ring has characteristic zero and no annihilator except zero. The mode is a prime, 2. Therefore, Theorem 4 is applicable.

Again denote the class of all rings with characteristic $v$ by $A_v$.

**Theorem 5:** A ring $R$ of $A_0$ has a minimal extension $G$ in the set $A_0$ iff the mode of $R$ is zero or 1. If $v > 0$ and $R \not\in A_v$, let $\delta$ be the least member of the set $D$ of positive integers $u$ which have a $u$-fier of $R$ of order $v/u$. The ring $R$ of $A_v$ has a minimal extension $G$ in $A_v$ iff $(\delta, \lfloor v/\delta \rfloor) = 1$. (iii)

**Proof:** The first part follows from Theorem 3 since $R \in A_0$ and $R \not\in F \rightarrow F \in A_0$.

Turning to the second part, assume $v > 0$. The set $D$ is non-empty for it contains the integer $v$ which has the $\lfloor v/\delta \rfloor$-fier 0 of order $v/\lfloor v/\delta \rfloor$. Hence $D$ contains a least member $\delta$ which is unique for $R$, and the $R$ of $A_v$ has at least one $\delta$-fier $d$ of order $v/\delta$.

To show (iii) is necessary, we shall assume there is a ring $G$ of $A_v$ which has unit and contains $R$. We shall also
assume for each ring $F$ of $A_v$ which has unit and contains $R$ there is a ring $G'$ in $A_v$ such that $G \cong G' \subseteq F$. For this ring $G$, there is by Theorem 2 a ring $G_1$ in $A_v$ such that (ii) holds with $\nu = \nu_G$. We show next that $\nu = \sigma$. By K), $R^*(d,\delta) \in A_v$. So by hypothesis this is a ring $G'$ such that $G \cong G' \subseteq R^*(d,\delta)$.

Combining this with (ii) we have $R^*(d,\delta)$ containing a strict isomorph of $R^*(\nu_e, \nu^e)$. It follows from Lemma 1 and D) that $\sigma = \lambda \nu_r$.

But since $\nu$ divides $v$ by N), it is a consequence of G) that $\Delta_{\nu_e} = v/\nu$ so $\nu \in D$. Hence $0 < \delta \leq \nu$ so $\lambda = 1$ and $\nu = \sigma$.

We now observe since $R^*(0,v) \in A_v$ by K), there exists by hypothesis a ring $G_0$ for which $G \cong G_0 \subseteq R^*(0,v)$. Combining this with (ii) and applying Lemma 1, we have that $I/(v)$ contains a strict isomorph of $I/(\nu_r)$. But since $\nu = \sigma$, this implies $(\sigma, v/\sigma) = 1$.

To prove (iii) is sufficient we first present the following lemma.
**Lemma 3:** If \( \pi \in D \) and \((d, \nu/d) = 1\) then \(d|\nu\).

**Proof:** Since \( \nu \in D \) has a \( \pi \)-fier of order \( \nu/\pi \), this implies \( \nu|\pi \). Also \( d|\nu \), so the only possible prime factor of \( \nu \) or of \( d \) are the prime factors of \( \nu \). Suppose \( \nu \) is not a multiple of \( \delta(\pi) \). Then there exists at least one prime \( \pi \) occurring to a higher power in \( d \) than in \( \nu \). Since \((d, \nu/\delta) = 1\), \( v = \pi^\alpha v_1; \delta = \pi^\alpha \delta_1; \nu = \pi^\beta \nu_1 \), where \( v_1, \delta_1, \) and \( \nu_1 \) are all prime to \( \pi \) and \( \alpha > \beta \geq 0 \). Furthermore \( v_1 \) is divisible by \( \delta_1 \) and \( \nu_1 \). Let \( \sigma, \tau, \phi, \psi \) be integers satisfying

\[
\begin{align*}
\sigma \pi^\alpha &
= 1(v_1) \\
\tau v_1 &
= 1(\pi^\infty)
\end{align*}
\]

(iv) \( \phi \tau \nu_1 v_1/\delta_1 \equiv 1(\pi^{\alpha-\phi}) \)
(v) \( \psi \sigma \pi^{\alpha-\phi-\tau} \equiv 1(v_1/\delta_1) \)

Now let \( d \) be a \( \delta \)-fier of \( R \) of order \( v/\delta \) and \( c \) a \( \nu \)-fier of order \( v/\nu \). We shall show that \( a = \phi \tau v_1c \psi \sigma \pi^\alpha d \) is a \( \pi^\beta \delta_1 \)-fier of order \( v/(\pi^\beta \delta_1) \). By G), the order of \( \phi \tau v_1c \) is \( \pi^{\alpha-\phi} \) and the order of \( \psi \sigma \pi^\alpha d \) is \( v_1/\delta_1 \). Hence by F), the order of \( a \) is \( \pi^{\alpha-\phi} v_1/\delta_1 = v/\pi^\beta \delta_1 \). Also if \( r \in (\pi) \),
(vi) $ar = ra = ( \phi T v_1 \psi + \psi \sigma \pi \delta ) r$. If we let $w = \phi T v_1 \psi_1 / \delta_1 + \psi \sigma \pi \alpha - \beta$, we see from (iv) $w \equiv 1(\pi \alpha - \beta)$ and from (v) $w \equiv 1(\pi \alpha - \beta v_1) / \delta_1$. If follows that $\phi T v_1 \psi + \psi \sigma \pi \delta \equiv \pi \delta_1 (v)$. Now since $v$ is the characteristic of $R$, this combined with (vi) shows $a$ is a $\pi \delta_1$-fier of $R$. We also know that $a$ has order $v / \pi \delta_1$ so $\pi \delta_1 \in D$. But since $\pi \delta_1 < \delta$ this contradicts the minimality of $\delta$ and establishes our indirect proof. Therefore, $\nu \sigma$ is a multiple of $\delta$.

We shall now prove sufficiency for Theorem 5. Assume (iii). Since we assume the existence of a $\delta$-fier $d$, clearly $k / \delta$. But since the order of $d$ is assumed to be $v / \delta$, we have $\delta | v$ which implies $(k, v / \delta) = 1$. Thus the $\delta$-fier is unique by $J$). We shall show $R^*(d, \delta)$ which belongs to $A_v$ by $k$ is our required ring.

If $F$ is a ring of $A_v$ with unit $e$ which contains $R$, then by Theorem 2 $F$ contains a strict isomorph of $R^*(\nu e, \nu \sigma)$ where in the notation of $N$, $\nu \sigma = \nu F$ and $\nu \sigma / v$. 
Evidently \( \omega e \) is a \( \gamma \)-flier of \( R \) of order \( \nu/\gamma \) by \( G \), so \( \omega e \in D \), and by Lemma 3, \( \gamma = \omega \delta \). But by \( G \), \( \Theta d \) is also a \( \gamma \)-flier of \( R \) of order \( \nu/\gamma \). It follows from \( J \) that \( \omega e = \Theta d \) since \( (iii) \) implies \( (k, \nu/\gamma) = 1 \).

Hence \( R^*(\omega e, \gamma) \) is identical to \( R^*(\Theta d, \omega \delta) \).

Since \( (iii) \) implies \( (\delta, \Theta) = 1 \), it follows from Lemma 2 that \( R^*(\Theta d, \omega \delta) \) contains a strict isomorph of \( R^*(d, \delta) \). Hence \( F \) contains a strict isomorph of the fixed ring \( R^*(d, \delta) \) which is the required minimal extension of \( R \) in \( A_\nu \).

**Corollary 1:** A ring \( R \) for which \( k = \nu \) has the ring \( R^*(0, \nu) \) as a minimal extension in \( A_\nu \).

**Corollary 2:** If the positive characteristic \( \nu \) of \( R \) is a product of distinct primes then \( R \) has a minimal extension in \( A_\nu \).

We shall end with one last example:

If \( R \) is the ideal \( \bar{2} \) in \( I/(48) \) then \( \nu = 24 \), \( k = 2 \), \( \delta = 8 \). Therefore \( (iii) \) is satisfied and \( \bar{32} \) is the unique \( 8 \)-flier of order \( 3 \).
FOOTNOTES


BIBLIOGRAPHY


