# A SYSTEM OF CANONICAL FORMS FOR RINGS ON A DIRECT SUM OF TWO INFINITE CYCLIC GROUPS 

Burnett R. Toskey

In this paper we canonically represent the isomorphism classes of all rings whose additive group is a direct sum of two infinite cyclic groups by a system of 4 by 2 matrices whose elements are rational integers. It is then shown how the canonical forms can be used to solve other problems relating to these rings. The results obtained are (1) that any integral domain in this class of rings is isomorphic to a quadratic extension of a subring of the integers, (2) the complete survey of rings in the class under study which are decomposable as a direct sum, and (3) the complete survey of rings in this class which are decomposable as an ordered product which is not a direct sum. The paper concludes with a description of other problems which can be solved by means of the canonical matrices using routine calculations.

Let $\left\{u_{1}\right\}$, and $\left\{u_{2}\right\}$ be infinite cyclic groups. Multiplication in a ring, $G$, whose additive group is $\left\{u_{1}\right\} \oplus\left\{u_{2}\right\}$ is determined by a matrix:

$$
\left(g_{i j k}\right)=\left(\begin{array}{ll}
g_{111} & g_{112} \\
g_{121} & g_{122} \\
g_{211} & g_{212} \\
g_{221} & g_{222}
\end{array}\right)
$$

where $u_{i} \cdot u_{j}=g_{i j 1} u_{1}+g_{i{ }_{j 2}} u_{2}, i, j=1,2$, and the $g_{i j k}$ are integers. If $G$ is associative, then the equality:

$$
g_{i j 1} g_{1 k p}+g_{i j 2} g_{2 k p}=g_{j k 1} g_{i 1 p}+g_{j k 2} g_{i 2 p}
$$

holds for $i, j, k, p=1,2$ (see [1]).
We consider the set of matrices of the above from which represent associative rings and reduce them to a system of canonical forms which represent the isomorphism classes of the rings. Our main tool in performing this reduction is the following result, which is a special case of the main result appearing in [7], and also a special case of a theorem of Beaumont (see Theorem 5 in [2]):

Theorem. If $G$ and $H$ are rings with multiplication determined by the matrices $\left(g_{i j k}\right)$ and $\left(h_{i j k}\right)$ respectively, then $G$ and $H$ are isomorphic if and only if there is a 2 by 2 matrix, $A$, with integer
entries, such that $|A|^{2}=1$ and $(A \otimes A)\left(g_{i j k}\right)=\left(h_{i j k}\right) A$.
When we have obtained the desired canonical forms, we shall use them to derive various properties of the rings under study.
2. The canonical forms. Our main result, upon which all subsequent results are based, is the following:

Theorem. Let matrices $N_{1}(x), N_{2}(x)$ and $C(x, y, z)$ be defined by:

$$
N_{1}(x)=\left(\begin{array}{cc}
x & 0 \\
0 & x \\
0 & 0 \\
0 & 0
\end{array}\right) \quad N_{2}(x)=\left(\begin{array}{cc}
x & 0 \\
0 & 0 \\
0 & x \\
0 & 0
\end{array}\right) \quad C(x, y, z)=\left(\begin{array}{cc}
x & z \\
y & 0 \\
y & 0 \\
0 & y
\end{array}\right)
$$

where $x, y, z$ are integers. Let $N_{1}=\left\{N_{1}(x): x>0\right\}, N_{2}=\left\{N_{2}(x): x>0\right\}$,

$$
\begin{aligned}
& C_{1}=\{C(0,0, z): z \geqq 0\}, \\
& C_{2}=\{C(x, 0, z): 0 \leqq z \leqq x / 2<x\}, \\
& C_{3}=\{C(x, y, z): 0 \leqq x \leqq y, y \neq 0\}
\end{aligned}
$$

and let $S=N_{1} \cup N_{2} \cup C_{1} \cup C_{2} \cup C_{3}$. Then every ring whose additive group is a direct sum of two infinite cyclic groups is isomorphic to a ring whose multiplication coefficients are given by a member of $S$ and no two members of $S$ can represent the multiplication coefficients of isomorphic rings.

Proof. A. Let $G$ be a noncommutative ring with multiplication given by the matrix $\left(g_{i j k}\right)$, so that we must have either $g_{121} \neq g_{211}$ or $g_{122} \neq g_{212}$. The associativity conditions are:

1. $g_{112}=g_{221}=g_{122} g_{121}=g_{211} g_{212}=0$
2. $g_{121}\left(g_{121}-g_{222}\right)=g_{122}\left(g_{122}-g_{111}\right)=0$ $g_{211}\left(g_{211}-g_{222}\right)=g_{212}\left(g_{212}-g_{111}\right)=0$.
3. $g_{121}\left(g_{212}-g_{111}\right)=g_{211}\left(g_{122}-g_{111}\right)$ $g_{122}\left(g_{222}-g_{211}\right)=g_{212}\left(g_{222}-g_{121}\right)$.
Since $g_{121} \neq 0$ implies $g_{121}=g_{222}, g_{122} \neq 0$ implies $g_{122}=g_{111}, g_{211} \neq 0$ implies $g_{211}=g_{222}, g_{212} \neq 0$ implies $g_{212}=g_{111}, g_{121}=g_{211}$ implies $g_{121}=g_{211}=g_{222}=0$, and $g_{122}=g_{212}$ implies $g_{122}=g_{212}=g_{111}=0$, there are two cases to consider:

Case 1. $\quad g_{111}=g_{122}, g_{211}=g_{222}, g_{121}=g_{212}=0$. Set $x=\left(g_{111}, g_{211}\right), g_{211}=$ $-c x, g_{111}=d x$, and let $a d-b c=1, A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$. Thus $(A \otimes A)\left(g_{i j k}\right)=$ $N_{1}(x) A$.

Case 2. $g_{111}=g_{212}, g_{121}=g_{222}, g_{122}=g_{211}=0$. As before, set $x=$ $\left(g_{121}, g_{111}\right), g_{121}=-c x, g_{111}=d x, \mathrm{ad}-b c=1, A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$, and we obtain $(A \otimes A)\left(g_{i j k}\right)=N_{2}(x) A$.

Hence every noncommutative ring on a direct sum of two infinite cyclic groups is isomorphic to a ring whose multiplication coefficients are given by member of $N_{1} \cup N_{2}$. We show next that no two of these can represent isomorphic rings.
(1) If either $(A \otimes A) N_{1}(r)=N_{1}(s) A$ or $(A \otimes A) N_{2}(r)=N_{2}(s) A$, where $A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$ and $|A|^{2}=1$, we obtain $c^{2} r=0$ and $a^{2} r=$ as, so that $|A|=a d$. Thus $a^{2}=1$ and $r=a s$. Finally, since $r$ and $s$ are both positive, we obtain $a=1, r=s$.
(2) If $(A \otimes A) N_{1}(r)=N_{2}(s) A$, where $A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$, we obtain $c^{2} r=$ $a d r=0$, which implies $c=a d=0$, so that $|A|=0$.

Hence no two members of $N_{1} \cup N_{2}$ can represent the coefficients of isomorphic rings. It is elementary to verify that the cofficients given by the matrices $N_{1}(x)$ and $N_{2}(x)$ satisfy the associativity conditions.
B. Let $G$ be a commutative ring with multiplication given by the matrix $\left(g_{i j k}\right)$, so that we must have $g_{121}=g_{211}$ and $g_{122}=g_{212}$. The associativity conditions reduce to:

1. $g_{121} g_{122}=g_{12} g_{221}$
2. $g_{121}\left(g_{121}-g_{222}\right)=g_{221}\left(g_{111}-g_{122}\right)$ $g_{122}\left(g_{122}-g_{111}\right)=g_{112}\left(g_{222}-g_{121}\right)$.
We first show that $G$ must be isomorphic to a ring with coefficients given by a matrix of the form $C(x, y, z)$. We have three cases to consider.

Case 1. If $g_{112}=g_{122}=g_{221}=0$, the associativity conditions reduce to $g_{121}\left(g_{121}-g_{222}\right)=0$. If $g_{121}=g_{222}$, the matrix for $G$ is already in the form $C\left(g_{111}, g_{121}, 0\right)$. If $g_{121} \neq g_{222}$, then we must have $g_{121}=0, g_{222} \neq 0$, so that we may let $\left(g_{111}, g_{222}\right)=r, g_{111}=d r, g_{222}=c r$, and find $a$ and $b$ such that $a d-b c=1$. If $A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$, we obtain the desired result: $(A \otimes A)\left(g_{i j k}\right)=C(a d r+b c r, c d r,-a b r) A$.

Case 2. If $\left(g_{112}, g_{122}\right)=r \neq 0$, let $g_{112}=-d r, g_{122}=c r, a d-b c=1$, and $A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$ we obtain $(A \otimes A)\left(g_{i j k}\right)=C(x, y, z) A$, where

$$
\begin{aligned}
& x=d\left(a^{2} g_{111}+2 a b g_{121}+b^{2} g_{221}\right)-c\left(+a^{2} g_{112}+2 a b g_{122}+b^{2} g_{222}\right) \\
& y=a c d g_{111}+d(a d+b c) g_{121}+b d^{2} g_{221}-b c^{2} g_{122}-b d c g_{222}
\end{aligned}
$$

$$
z=-b\left(\alpha^{2} g_{111}+2 a b g_{121}+b^{2} g_{221}\right)+a\left(a^{2} g_{112}+2 a b g_{122}+b^{2} g_{222}\right)
$$

Case 3. If $g_{112}=g_{122}=0, g_{221} \neq 0$, let $B=\left(\begin{array}{ll}0 & 1 \\ 1 & 0\end{array}\right)$ so that

$$
(B \otimes B)\left(g_{i j k}\right)=\left(h_{i j k}\right) B,
$$

and $h_{112}=g_{221}$, and we may apply the transformation of Case 2 to the matrix $\left(h_{i j k}\right)$.

Thus we have shown that every commutative ring is isomorphic to a ring with multiplication coefficients given by a matrix of the form $C(x, y, z)$. Again, it is elementary to see that every matrix of the form $C(x, y, z)$ represents the multiplication coefficients of an associative ring. We now assume that the ring $G$ has coefficients given by $C(x, y, z)$ for our final reduction to canonical form. There are three cases to consider.

Case 1. If $x=y=0$, then if $z \geqq 0, C(x, y, z) \in C_{1}$, and if $z<0$, let $A=\left(\begin{array}{rr}-1 & 0 \\ 0 & -1\end{array}\right)$ and we obtain $(A \otimes A) C(0,0, z)=C(0,0,-z) A$, and $C(0,0,-z) \in C_{1}$.

Case 2. If $x \neq 0, y=0$, let $a=|x||x, z=b| x \mid+r$, where $0 \leqq r<|x|$, and $A=\left(\begin{array}{ll}a & b \\ 0 & 1\end{array}\right)$ so that $|A|^{2}=a^{2}=1$. We obtain

$$
(A \otimes A) C(x, 0, z)=C(|x|, 0, r) A
$$

If $0 \leqq r \leqq|x| / 2$, then $C(|x|, 0, r) \in C_{2}$. If $1 / 2|x| \leqq r<|x|$, let $B=$ $\left(\begin{array}{rr}1 & 1 \\ 0 & -1\end{array}\right)$ and we obtain $(B \otimes B) C(|x|, 0, r)=C(|x|, 0,|x|-r) B$, and $C(|x|, 0,|x|-r) \in C_{2}$.

Case 3. If $y \neq 0$, let $d=|y| / y, x=b(-2 y)+r$, where $0 \leqq r<$ $|2 y|$, and $A=\left(\begin{array}{ll}1 & b \\ 0 & d\end{array}\right)$ so that $|A|^{2}=d^{2}=1$. We obtain $(A \otimes A) C(x, y, z)=$ $C(r,|y|, t) A$, where $t=d z-b d x-b^{2}|y|$. If $0 \leqq r \leqq|y|$, then $C(r,|y|, t) \in C_{3}$. If $|y| \leqq r<2|y|$, let $B=\left(\begin{array}{rr}-1 & 1 \\ 0 & 1\end{array}\right)$, and we have $(B \otimes B) C(r,|y|, t)=C(2|y|-r,|y|, r+t-|y|) B$, and

$$
C(2|y|-r,|y|, r+t-|y|) \in C_{3} .
$$

Hence every commutative ring on a direct sum of two infinite cyclic groups is isomorphic to a ring whose multiplication coefficients are given by a member of $C_{1} \cup C_{2} \cup C_{3}$. Since no member of $N_{1} \cup N_{2}$ can represent a ring which is isomorphic to any member of $C_{1} \cup C_{2} \cup C_{3}$, the proof of the theorem will be completed by showing that no two members of $C_{1} \cup C_{2} \cup C_{3}$ can represent isomorphic rings. In the follow-
ing, $A=\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$.
(1) Suppose $(A \otimes A) C_{1}(0,0, z)=C_{1}(0,0, v) A$ with $|A|^{2}=1$. We then have $v c=c^{2} z=0, a^{2} z=v d$. Hence if $z=0$, we must have $v=$ 0 , and if $z>0$, we obtain $c=0, a^{2}=d^{2}=1$, and therefore $z=v d$. Since $v>0$, we have $d=1, z=v$.
(2) Suppose $(A \otimes A) C_{1}(0,0, z)=C_{2}(x, 0, v) A$, so that $c^{2} z=a x+$ $v c=0$ and $a^{2} z=b x+v d$. If $z=0$, we have $|A|=0$, since $x \neq 0$, and if $z>0$, we have $c=a=0$ and again obtain $|A|=0$.
(3) Suppose $(A \otimes A) C_{1}(0,0, z)=C_{3}(x, y, v) A$. But then $a y=c y=$ 0 , and hence $a=c=0$ and $|A|=0$.
(4) Suppose $(A \otimes A) C_{2}(x, 0, z)=C_{2}(u, 0, v) A$ and $|A|^{2}=1$. Then $c^{2} x=0, a^{2} x=a u+v c, a^{2} z=b u+v d$. Hence $c=0$, and $a^{2}=d^{2}=1$, $x=a u, z=b u+v d$, and we must have $a=1, x=u$, since $x>0$ and $u>0$. But now $0 \leqq b u+v d \leqq u / 2$, so that if $d=1$ we must have $b=0, z=v$, and if $d=-1$ we must have either $b=0$, in which case $z=v=0$, or $b=1$, in which case $z=v=u / 2$.
(5) Suppose $(A \otimes A) C_{2}(x, 0, z)=C_{3}(u, y, v) A$, so that we have $a c x=y a, c^{2} x=c y, a c z=y b, \quad c^{2} z=d y$. If $c=0$, we obtain $a=0$, since $y \neq 0$, and $|A|=0$. If $c \neq 0$, then $y=c x, a z=b x, c z=d x$ and hence $|A|=0$, since $x \neq 0$.
(6) Suppose $(A \otimes A) C_{3}(x, y, z)=C_{3}(u, v, w) A$ and $|A|^{2}=1$. We obtain the equations:

$$
\left\{\begin{array} { l } 
{ a ^ { 2 } x + 2 b c y = a u + c w } \\
{ a c x + ( a d + b c ) y = a v } \\
{ c ^ { 2 } x + 2 c d y = c v }
\end{array} \quad \left\{\begin{array}{l}
a^{2} z+b^{2} y=b u+d w \\
a c z+b d y=b v \\
c^{2} z+d^{2} y=d v
\end{array}\right.\right.
$$

If $c \neq 0$, we obtain $v=c x+2 d y$, so that $c(a z-b x)=b d y$ and $c(c z-d x)=d^{2} y$, yielding $z=0$ so that $v=d y, c x+d y=0$ and finally $b c y=a d y$ and $|A|=0$. Hence we must have $c=0, a^{2}=d^{2}=1$. This yields $x=a u, v=d y$ so that $a=d=1, x=u, v=y$, and $z+$ $b^{2} y=b u+w$. By symmetry, $w+k^{2} v=k x+z$. But this implies $(b+k) x=\left(b^{2}+k^{2}\right) y$, so that either $b=0$, or $k=0$, or $b=k=1$, $x=y$. In any case, we obtain $z=w$.

Hence no two members of $C_{1} \cup C_{2} \cup C_{3}$ can represent the coefficients of isomorphic rings, and the proof of the theorem is complete.

We conclude this section by remarking that the algebra types (see [3], page 61) of the rings can be determined from the canonical forms. Types I, II, III, IV, and V refer to [3], page 97:
(i) Any ring represented by a member of $N_{1}$ has algebra type II.
(ii) Any ring represented by a member of $N_{2}$ has algebra type III.
(iii) Any ring represented by a member of $C_{1}$ has algebra type $V$ if $z>0$ and nil algebra type if $z=0$.
(iv) Any ring represented by a member of $C_{2}$ has algebra type I.
(v) Any ring represented by $C_{3}$ with $x^{2}+4 y z=0$ has algebra type IV.
(vi) Any ring represented by $C_{3}$ with $x^{2}+4 y z=v^{2} \neq 0$ has type $R \oplus R$ (semi-simple type).
(vii) Any ring represented by $C_{3}$ with $x^{2}+4 y z$ not the square of an integer has quadratic field type.

This last result is a corollary of the first result in the following section. Rings in different classes from the above list are not quasiisomorphic, since quasi-isomorphic rings have the same algebra type.
3. Relationship to known rings. Let $C(r)$ denote the ring whose additive group is the infinite cyclic group $\{u\}$, with multiplication defined by $u u=r u$. Since $C(r)$ and $C(s)$ are isomorphic if and only if $r^{2}=s^{2}$, we may assume $r \geqq 0$. Also, if $r>0$, then $C(r)$ is isomorphic to the subring of the integers generated by $r$ and $C(0)$ is the zero ring with infinite cyclic additive group. If $C(r)$ and $C(s)$ are two of these rings (not necessarily distinct), then the direct sum and the ordered product (see [6]) are rings whose additive group is the direct sum of two infinite cyclic groups. If $\alpha$ is a root of a quadratic equation which is irreducible over the ring of integers, then the subring of the field of complex numbers generated by $\alpha$ and $C(r), r>0$, considered as a subring of the ring of integers, will have the direct sum of two infinite cyclic groups as its additive group, if and only if $\alpha$ is a zero of a quadratic polynomial, irreducible over the integers, of the form $X^{2}+n X+m$, where $n, m$ are integers. In this section we shall use the canonical forms which were obtained in the previous section to express the rings of the three types mentioned above.

Our first result is the following, which shows that any integral domain whose additive group is the direct sum of two infinite cyclic groups is isomorphic to a quadratic extension of a subring of the integers. It is a refinement of a special case of a theorem by Beaumont and Wisner (Theorem 3, in [4]).

Theorem. The following are equivalent:

1. $C_{3}(x, y, z)$ is an integral domain.
2. $x^{2}+4 y z$ is not the square of a rational integer.
3. $C_{3}(x, y, z)$ is isomorphic to the subring of the complex numbers generated by $C(y)$ and $\alpha$, where $\alpha^{2}-x \alpha-y z=0$.

Proof. (1) implies (2): Suppose $x^{2}+4 y z=v^{2}$. If $z \neq 0$, then $\left[(x-v) u_{1}+2 z u_{2}\right] \cdot\left[2 y u_{1}+(v-x) u_{2}\right]=0$, and if $z=0$, we have

$$
\left(y u_{1}-x u_{2}\right)\left(u_{1}\right)=0
$$

so that in either case $C_{3}(x, y, z)$ is not an integral domain.
(2) implies (3): It is easy to verify that the correspondence $a u_{1}+$ $b u_{2} \rightarrow a \alpha+$ by is the required isomorphism.

Since it is evident that (3) implies (1), the proof of the theorem is complete.

Our theorem on the canonical forms and the above theorem may be combined to yield the following:

Corollary. For rational integers $x, y$, and $z$, let $\alpha_{1}(x, y, z)$ and $\alpha_{2}(x, y, z)$ denote the zeros of the polynomial $\alpha^{2}-x \alpha-y z$, let $D(x, y, z)$ denote the subring of the complex numbers which is generated by the subring $C(y)$ of the rational integers and $\alpha_{1}(x, y, z)$ and let $D=\left\{D(x, y, z): 0 \leqq x \leqq y, y \neq 0\right.$, and $x^{2}+4 y z$ not the square of a rational integer $\}$. Then every subring of the complex numbers which is generated by a subring of the rational integers and a zero of a monic quadratic polynomial which is irreducible over the ring of rational integers is isomorphic to a member of $D$ and no two distinct members of $D$ are isomorphic.

Turning next to the problem of decomposability, we first note that if a ring whose additive group is the direct sum of two infinite cyclic groups decomposes as the direct sum of two ideals, then the additive groups of the direct summands must be cyclic, and hence the ring must be commutative. Since an integral domain cannot decompose, we need only consider the rings $C_{1}(0,0, z), C_{2}(x, 0, z)$ and those rings $C_{3}(x, y, z)$ for which $x^{2}+4 y z=v^{2}$ for some rational integer, $v$. The following result therefore gives a survey of the docomposable rings on a direct sum of two infinite cyclic groups:

## Theorem.

A. $C_{1}(0,0, z)$ is decomposable if and only if $z=0$.
B. $C_{2}(x, 0, z)$ is decomposable if and only if $z=0$.
C. If $x^{2}+4 y z=v^{2}, v \geqq 0, v$ a rational integer, then $C_{3}(x, y, z)$ is decomposable if and only if $(v-x, 2 y)(v+x, 2 y)=4 y v$.

Proof. A. $C_{1}(0,0,0)$ is just the zero ring, and hence $C_{1}(0,0,0)=$ $C(0) \oplus C(0)$. If $z \neq 0$ and $\left\{a u_{1}+b u_{2}\right\}$ is an ideal in $C_{1}(0,0, z)$, then we must have $u_{1}\left(a u_{1}+b u_{2}\right)=a z u_{2}=a r u_{1}+b r u_{2}$ for some $r$. But this
implies $a r=0, a z=b r$ and since $z \neq 0$, we must have $a=r=0$, if the ideal is not the zero ideal. Hence the only proper ideals are of the form $\left\{b u_{2}\right\}$, and $u_{1}$ is not contained in the sum of any two of these, and hence $C_{1}(0,0, z)$ is indecomposable.
B. It is easy to check that $C_{2}(x, 0,0)=\left\{u_{1}\right\} \oplus\left\{u_{2}\right\}$. If $z \neq 0$ and $\left\{a u_{1}+b u_{2}\right\}$ is an ideal in $C_{2}(x, 0, z)$, then we must have $u_{1}\left(a u_{1}+b u_{2}\right)=$ $\alpha x u_{1}+\alpha z u_{2}=\alpha r u_{1}+b r u_{1}$ for some $r$. This implies $a x=a r, \alpha z=b r$, so that either $a=r=0$, or $a b \neq 0, x=r$, and $a z=b x$. As before, $C_{2}(x, 0, z)$ cannot decompose as the sum of two ideals of the form $\left\{c u_{2}\right\}$, and two ideals of the form $\left\{a u_{1}+b u_{2}\right\}$ with $a b \neq 0$ will not be disjoint because of the condition $a z=b x$. But if we suppose $C_{2}(x, 0, z)$ decomposes as the sum of $\left\{a u_{1}+b u_{2}\right\}$ and $\left\{c u_{2}\right\}$ then we must have $u_{1}=k a u_{1}$ for some $k$, so that $\alpha^{2}=1$ and $z=a b x$, contrary to the condition $0 \leqq z \leqq x / 2<x$.
C. First suppose $C_{3}(x, y, z)=\left\{a u_{1}+b u_{2}\right\} \oplus\left\{c u_{1}+d u_{2}\right\}$. Since no ideal can be of the form $\left\{b u_{2}\right\}, b \neq 0$, we can assume $a>0$ and $c>0$. Since $u_{1}, u_{2} \in C_{3}(x, y, z)$, there must exist integers $n, m, p, q$ such that $1=n a+m c, 0=n b+m d, \quad 0=p a+q c$, and $1=p b+q d$. This implies $(a d-b c)^{2}=1$. Hence $(a, b)=(c, d)=1$. We must also have $v_{u_{1}}\left(a u_{1}+b u_{2}\right)=(a x+b y) u_{1}+a z u_{v_{2}}=t a u_{1}+t b u_{2}$, whence, eliminating $t$, we obtain $b / a=(-x \pm v) /(2 y)$, and similarly for $d / c$. Since $b / a \neq d / c$, we can assume $2 y=a(v-x, 2 y)=c(v+x, 2 y), v-x=b(v-x, 2 y)$ and $v+x=-d(v+x, 2 y)$, and finally

$$
\begin{aligned}
(v-x, 2 y)(v+x, 2 y) & =(a d-b c)^{2}(v-x, 2 y)(v+x, 2 y) \\
& =(a d-b c)(-4 y v)
\end{aligned}
$$

and hence, since $y>0, v \geqq 0$, we must have $a d-b c=-1$. Conversely, if we assume $(v-x, 2 y)(v+x, 2 y)=4 v y$, let

$$
2 y=a(v-x, 2 y)=c(v+x, 2 y), v-x=b(v-x, 2 y)
$$

and $v+x=-d(v+x, 2 y)$, and it is easy to check that $a d-b c=-1$ and $C_{3}(x, y, z)=\left\{a u_{1}+b u_{2}\right\} \oplus\left\{c u_{1}+d u_{2}\right\}$.

The problem of decomposability as an ordered product of two subrings of the integers is somewhat simpler. If $C(r)$ and $C(s)$ are two subrings of the integers, and an ordered product $C(r)(<) C(s)$ is not a ring direct sum, then it is easy to verify that it is a ring with additive group which is a direct sum of two infinite cyclic groups with multiplication coefficients given by the matrix: $\left(\begin{array}{ll}r & 0 \\ s & 0 \\ s & 0 \\ 0 & s\end{array}\right)$, which
may be transformed to a member of $C_{3}$, by letting $r=2 b s-t$, with $0 \leqq t<2 s$, and applying the matrix $A=\left(\begin{array}{rr}1 & -b \\ 0 & 1\end{array}\right)$ to obtain

$$
C^{3}\left(t, s, b t+b^{2} s\right)
$$

if $0 \leqq t<s$, or the matrix $B=\left(\begin{array}{rc}-1 & b+1 \\ 0 & 1\end{array}\right)$ to obtain

$$
C_{3}\left(2 s-t, s,(-1-b)(2 s-t)+(-1-b)^{2} s\right)
$$

if $s \leqq t<2 y$. Thus the ordered product is isomorphic to a ring of the form $C_{3}(x, y, z)$, with $z=c x+c^{2} y$. Conversely, the matrix $\left(\begin{array}{ll}1 & c \\ 0 & 1\end{array}\right)$ may be applied to the ring $C_{3}\left(x, y, c x+c^{2} y\right)$ to obtain the ordered product $C(|x+2 c y|)(<) C(y)$. The condition $z=c x+c^{2} y$ is equivalent to $x^{2}+4 y z=(x+2 y c)^{2}$ so that the rings are not integral domains, and we must have either $2 y \mid v-x$ or $2 y \mid v+x$, where $x^{2}+4 y z=v^{2}$. This proves the following:

Theorem. A. No member of $N_{1} \cup N_{2} \cup C_{1} \cup C_{2}$ can represent the multiplication coefficients of an ordered product of two rings which is not the direct sum.
B. $C_{3}(x, y, z)$ represents the multiplication coefficients of an ordered product of two rings which is not a direct sum if and only if $x^{2}+4 y z=v^{2}$ and either $2 y \mid v-x$ or $2 y \mid v+x$.
4. Concluding remarks. By using the canonical forms for the rings on a direct sum of two infinite cyclic groups, many other problems involving these rings may be solved by straightforward elementary calculations. We conclude the present paper by indicating some of these results, omitting the calculations.
A. A complete survey of nonzero idempotents is as follows: (a) The elements of the form $u_{1}+b u_{2}$ are left identities in $N_{1}(1)$ and right identities in $N_{2}(1)$. (b) $u_{1}$ is idempotent in $C_{2}(1,0,0)$, but not an identity. (c) $u_{2}$ is the identity in $C_{3}(x, 1, z)$. (d) $u_{1}$ is idempotent in $C_{3}(1, y, 0)$ and $-u_{1}+u_{2}$ is idempotent in $C_{3}(1,1,0)$; neither is an identity.
B. Since the additive group of any subring is either cyclic or is the direct sum of two infinite cyclic groups, we can find all subrings by calculating the images of isomorphisms on $C(r)$ or members of $C_{1} \cup C_{2} \cup C_{3} \cup N_{1} \cup N_{2}$ into the given ring. The subrings which are found may be tested directly to determine whether they are ideals. It can be shown, for example, that the class of rings $C_{1}(0,0, z)$, with $z>0$, have the property that each is isomorphic to an ideal of any
other member of the class. Other classes of rings in $C_{2} \cup C_{3}$ also have this property.
C. It can be easily shown for any ring on a direct sum of two infinite cyclic groups, using the canonical forms, that the prime radical, the Jacobson radical, and the McCoy radical coincide ([5], pages $69,112,132$, respectively), and hence they may be calculated as the maximal images of isomorphisms of $C(0)$ and $C_{1}(0,0, z)$ into the given ring, these being the only nilpotent rings with additive group either infinite cyclic or a direct sum of two infinite cyclic groups.
D. If a correspondence between any two of the rings is designated by $u_{i} \rightarrow a_{i 1} u_{1}+a_{i 2} u_{2}$, it is easy to determine the set of 2 by 2 matrices $\left(a_{i j}\right)$ which represent homomorphisms between the rings. The set of endomorphisms of a given ring can also be determined in this way, as well as the group of automorphisms. The automorphisms, for example, are as follows:
(a) For $N_{1}$ or $N_{2}$ : isomorphic to the multiplicative group of matrices of the form $\left(\begin{array}{ll}1 & b \\ 0 & d\end{array}\right)$ where $b$ is an integer and $d^{2}=1$.
(b) For $C_{1}(0,0,0)$ : the multiplicative group of all matrices of the form $\left(\begin{array}{ll}a & b \\ c & d\end{array}\right)$ with $a, b, c, d$ integers such that $(a d-b c)^{2}=1$; and for $C_{1}(0,0, z), z>0$ : The multiplicative group of matrices of the form $\left(\begin{array}{ll}a & b \\ 0 & 1\end{array}\right)$ with $b$ an integer and $a^{2}=1$.
(c) For $C_{2}(x, 0, z), C_{3}(x, x, z)$ and $C_{3}(0, y, z)$ : cyclic of order two. (d) $C_{3}(x, y, z), 0<x<y$ : the identity.

## References

1. Ross A. Beaumont, Rings with additive group which is the direct sum of cyclic groups, Duke Maith. J., 15 (1948), 367-369.
2. ——, Matric criteria for the uniqueness of basis number and the equivalence of algebras over a ring, Publicationes Mathematicae Debrecen 4, (1956), 469-480.
3. R. A. Beaumont and R. S. Pierce, Torsion-free rings, Illinois J. Math. 5 (1961), 61-98.
4. R. A. Beaumont and R. J. Wisner, Rings with additive group which is a torsionfree group of rank two, Acta Scientiarum Mathematicarum, Szeged, 20 (1959), 105116.
5. Neal H. McCoy, The Theory of Rings, Macmillan, New York, 1964.
6. Burnett R. Toskey, Ordered products of rings, Journal fur die reine und angewandte Mathematik 209, (1962), 163-166.
7. -, Rings on a direct sum of cyclic groups, Publicationes Mathematicae, Debrecen, 10 (1963), 93-95.

Received June 6, 1965.
Seattle University
Seattle, Washington

