12-1997

Structure in Zero-Divisor Graphs of Commutative Rings

Philip S. Livingston
University of Tennessee - Knoxville

To the Graduate Council:

I am submitting herewith a thesis written by Philip S. Livingston entitled "Structure in Zero-Divisor Graphs of Commutative Rings." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

David F. Anderson, Major Professor

We have read this thesis and recommend its acceptance:

Robert Daverman, Carl G. Wagner

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a thesis written by Philip S. Livingston entitled "Structure in zero-divisor graphs of commutative rings". I have examined the final copy of this thesis for form and content and recommend that it be acepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

David F Anderson

David F. Anderson, Major Professor

We have read this thesis
and recommend its acceptance:

[illegible]

Carl G. Wagner

Accepted for the Council:

[illegible]

Associate Vice Chancellor and
Dean of The Graduate School

STRUCTURE IN ZERO-DIVISOR GRAPHS OF COMMUTATIVE RINGS

A Thesis
Presented for the Master of Arts
Degree
The University of Tennessee, Knoxville

Philip Stephen Livingston
December 1997

DEDICATION

For my parents, Bob and Audrey, who opened my mind,

For Fumiko, who opened my eyes to the beauty of mathematical ideas,

For Dick, who showed me the depths of that beauty,

and

for Nancy, Natasha and Natalie.

ACKNOWLEDGMENTS

There are many people for whose encouragement and help I am grateful. I would like to mention especially my mentor and role model Professor David Anderson, whose example and energy kept me on track. In addition, Professors Carl Wagner, Robert Daverman, William Wade and Balram Rajput provided stimulating instruction and moral support. I should also like to give a special thanks to Samuel Jordan for his help in my negotiating difficult waters.

A unique thanks is owed to Dr. Richard Stafford for his timeless support and encouragement, and the use of his computer.

Lastly, to my wife Nancy, a great and humble debt of gratitude is owed for encouraging my return to the university and supporting me in the endeavor in countless ways.

ABSTRACT

In this research, we associate a graph in a natural way with the zero-divisors of a commutative ring. We endeavor to characterize various attributes of the graph, including connectivity, diameter, and symmetry. In exploring symmetry in the graph, we examine the automorphism group of the graph, and provide a complete characterization for the rings $\mathbb{Z}_N$. Secondly, we seek ring-theoretic properties which may be described in terms of the associated zero-divisor graph. These include, among other results, a strong relationship between finite local rings and graphs admitting a vertex connected to every other vertex.

PREFACE

In an introductory class in ring theory, one learns that the zero-divisor relation in a ring is not transitive. That is to say, for a commutative ring R and elements x, y, and z in R, the fact that $xy=0$ and $yz=0$ does not necessarily imply that $xz=0$. This statement is true even in the simplest of commutative rings. For example, consider the ring of integers modulo twelve, $\mathbb{Z}_{12}$. The following relations are immediate: $\mathbf{2 \bullet 6 = 0}$ and $\mathbf{6 \bullet 4 = 0}$, while $\mathbf{2 \bullet 4 \neq 0}$. One might ask, however, whether there is an underlying "organization" to the zero-divisors of a commutative ring. For example, how much does the relation deviate from being transitive? The zero-divisor relation lends itself to an immediate identification with a simple graph. In 1988, Istefan Beck [3] associated a graph with a commutative ring using the zero-divisor relation, and went on to explore colorings of the graph. We will attempt to describe more basic structure of these graphs, and hence develop a combinatorial and geometric description of the zero-divisors of a commutative ring.

TABLE OF CONTENTS

LIST OF FIGURES

I. Introduction

I.1 Graph-Theoretic Definitions

A (***simple***) ***graph*** $\Gamma = (V, E)$ is a set V, called the ***vertex*** set, and a set of irreflexive, symmetric relations E, on V, called the ***edge*** set. If x and y are distinct vertices of Γ, that is to say, $x, y \in V$ with $x \neq y$, then if x and y are related in E, we call the relation an ***edge*** between x and y, denoted by (x, y). Note that if (x, y) is an edge, then (y, x) denotes the same edge. With this in mind, we may be precise in our association of a graph with the zero-divisors of a ring:

Definition 1. Let R be a commutative ring with non-zero identity. We define the ***zero-divisor graph*** of R, denoted ***$\Gamma(R)$***, to be a simple graph with vertex set being the set of non-zero zero-divisors of R and with (x, y) an edge if and only if $x \neq y$ and $xy = 0$.

A word of explanation is in order. The authors ([1] and [3]) referenced in this paper have included all of the elements of R in the vertex set. From a perspective of trying to understand the structure of these graphs, the roles played by zero and the elements which are not zero-divisors add little. Zero is connected to everything and non-zero-divisors are connected to nothing but zero. We use the denotation ${}_0\Gamma(R)$ to indicate this more general case where necessary. If not explicitly stated, most of the results that follow extend in a natural way to the latter setting. Throughout, a ring R will always be commutative with non-zero identity. We will usually assume that the ring R is finite, and hence $\Gamma(R)$ is also finite.

It is necessary to introduce some key graph-theoretic definitions. A ***complete graph*** is a graph with edge set containing all possible edge relations on its vertices, and is denoted K_n, where n is the number of vertices. A ***subgraph*** of a graph is any subset of vertices together with any subset of edges containing those vertices. An ***induced subgraph*** is a subgraph maximal with respect to the number of edges. If an induced subgraph is itself complete, it is called a ***clique***. The number of vertices in a maximal clique of a graph Γ is denoted ***cl(Γ)***. If (x, y) is an edge we say that x and y are adjacent, and when convenient we will denote it by ***x-y***. A ***path*** of length n from a vertex x to a distinct vertex y is a sequence of n+1 distinct vertices $x = v_0, v_1, \ldots, v_n = y$ such that v_i and v_{i+1} are adjacent for $0 \leq i \leq n-1$. For clarity, we will usually denote such a path by $v_0 - v_1 - \ldots - v_n$. If x and y are vertices of a graph, we define the ***distance*** between x and y, d(x, y), to be the length of a shortest path between them. If no path exists between x and y, we say that $d(x, y) = \infty$. If in a graph Γ there are vertices x and y such that $d(x, y) = \infty$, we say that the graph is

disconnected. A ***component*** of Γ is a maximal connected subgraph. We define a *cycle* by requiring that $x = y$ in the above definition of a path. Note that for both the path and the cycle, the length is just the number of edges determined by the $\{v_i : 0 \leq i \leq n\}$. In particular, no cycle of shorter length may be determined by the $\{v_i : 0 \leq i \leq n\}$. In Figure 1, the sequence a-b-c is an example of a path of length 2, the sequence b-c-d-b defines a cycle of length three, and a-b-c-d-b is neither a cycle nor a path. (This last sequence is often referred to as a ***walk***. We will not make further use of this term.)

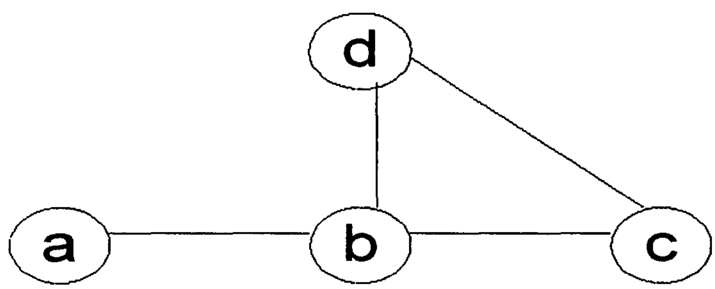


Figure 1: A Graph

A cycle of length three is commonly called a ***triangle***, a cycle of length four is a ***square***, and so on. Thus, the cycle b-d-c-b in the figure above is a triangle.

Two more definitions are central in characterizing a graph. The ***diameter*** of a graph Γ, denoted ***diam*** Γ, is defined to be the maximum of the distances d(x, y) as x and y vary over all vertices in the graph. The ***girth*** of a graph is the length of the shortest cycle. The graph in the figure above has diameter two and girth three.

I.2 Ring-Theoretic Definitions and Elementary Results

We shall make use of several definitions and general propositions from commutative ring theory, and we provide them here. First and foremost, the set $z(R) = \{x \in R \mid xy = 0 \text{ for some } 0 \neq y \in R\}$ is the ***set of zero-divisors*** of R. In particular, observe that $0 \in z(R)$, and, for example, if R is an integral domain, $|z(R)| = 1$. A ring is ***Noetherian*** if each of its ideals is finitely generated. If we consider the set of ideals under the partial order of inclusion, the ***height*** of a prime ideal is the length of the longest chain of prime ideals below it. Thus, for example, a prime ideal has height zero if no prime ideal is contained properly inside it. The ***dimension*** of a ring is the supremum of all heights of prime ideals. A ring is ***quasi-local*** if it contains a unique maximal ideal. In a commutative ring R, the ***annihilator*** (ideal) of an element x, denoted ***ann(x),*** is the set of those elements y for which xy = 0. In terms of the zero-divisor graph, this would be the set of vertices adjacent to x. Note that x itself may be an element of ann(x). This fact would not be apparent in the zero-divisor graph of R. The proof of the fact that ann(x) is an ideal is straight-forward and left to the reader. Another important ideal is the ***nil-radical*** of R, denoted ***nil(R)***. It is defined to be the set of nilpotent elements of R. The fact that this is an ideal is again straight-forward, and again left to the reader. Another important characterization of nil(R) is the fact [5, Theorem 25] that it is precisely the intersection of the prime ideals of R.

We will make use of the following proposition regarding finite rings.

Proposition 2. If a ring R is finite, then R is zero-dimensional and Noetherian.

Proof: For the first part, since a finite integral domain is a field, each prime ideal of R is maximal. Thus R is zero-dimensional. Clearly R is Noetherian. ■

Proposition 3. If a ring R is finite, then every element is a unit or a zero-divisor.

Proof: Suppose R has maximal ideals $M_1, \ldots, M_n$. Since $z(R) \subseteq M_1 \cup \ldots \cup M_n$ in every case, we need only to demonstrate the reverse inclusion.

Let $0 \neq x \varepsilon M_1$, and pick $y \varepsilon M_2 \cap \ldots \cap M_n \setminus M_1$ (if $n = 1$, let $y = 1$). Observe that y is not nilpotent since it misses M_1, and hence is not in nil(R). But $xy \varepsilon M_1 \cap \ldots \cap M_n = \text{nil}(R)$, and hence is nilpotent, so that $x^m y^N = 0$ for some $m \geq 1$ and $N \geq 1$, and $x^{m-1}y^N \neq 0$. Hence x is a non-zero zero-divisor, and hence $z(R) \subseteq M_1 \cup \ldots \cup M_n$. ■

Proposition 4. [5, Theorems 6 and 86] An annihilator which is maximal among annihilators is prime. If M is a maximal ideal in a finite ring R, there is some non-zero $x \in M$ with $xM = 0$.

Proof: Suppose ann(x) is maximal among annihilators, and let $ab \varepsilon$ ann(x). We must show that a or $b \varepsilon$ ann(x). Assume that $a \notin$ ann(x). Then $ax \neq 0$. Now ann(ax) $\supseteq$ ann(x), since anything which annihilates x also annihilates the element ax. Conversely, since ann(x) is maximal, ann(ax) $\subseteq$ ann(x). Hence, ann(ax) = ann(x). Since b annihilates ax it follows that $b \varepsilon$ ann(x). To prove the second part, note that M_M = ann(x/1) for some $x \varepsilon M$. Thus if M is finite, there exists an $s \varepsilon R\backslash M$ such that $sMx = 0$. Hence, we have M = ann(sx). ■

I.3 Some Preliminary Observations

A very general theorem is provided by Istefan Beck [3, Proposition 2.2].

Theorem 5. The following statements are equivalent for a ring R:

i) ${}_0\Gamma(R)$ is triangle-free.

ii) Either R is isomorphic to $\mathbb{Z}_2[X]/(X^2)$ or $\mathbb{Z}_4$, or R is an integral domain.

Proof: (Beck) Observe that i) $\Rightarrow$ ii), trivially. Suppose that ${}_0\Gamma(R)$ is triangle-free and is not an integral domain. Let $xy = 0$, where x and y are non-zero. Then $\{0, x, y\}$ is a clique. It follows that $x=y$. Thus $x \neq 0$ and $x^2 = 0$. The ideal xR is a clique and we conclude that $|xR| = 2$. Now assume that $z \in \mathrm{ann}(x)$. Then $\{0, x, z\}$ is a clique and therefore $z \in Rx = \{0, x\}$. Hence $\mathrm{ann}(x) = xR$. From the exact sequence

$$0 \to \mathrm{ann}(x) \to R \xrightarrow{x} xR \to 0$$

we conclude that $|R| = 4$. If the characteristic of R is 4 we have $R \approx \mathbb{Z}_4$, and if the characteristic of R is 2, we have $R \approx \mathbb{Z}_2[X]/(X^2)$. ■

In the context of the zero-divisor graph we have defined, one which excludes zero and units, we may add the following equivalence.

Theorem 6. The following statements are equivalent for a ring R:

i) ${}_0\Gamma(R)$ is triangle-free.

ii) Either R is isomorphic to $\mathbb{Z}_2[x]/(x^2)$ or $\mathbb{Z}_4$, or R is an integral domain.

iii) $\Gamma(R)$ consists of exactly a single point, or is empty.

<u>Proof</u>: ii) implies iii) is clear by inspection of the graphs.

iii) implies i) is clear: the addition of disconnected points and a zero-element connected to each point will not result in a triangle. ■

Thus, the only interesting cases arise when R is not an integral domain, and we will assume that this is the case throughout the rest of the paper. We are mainly interested in the case when $\Gamma(R)$ is finite and non-empty. We next show that this happens precisely when R is finite and not a field.

Theorem 7. Let R be a commutative ring. Then $1 \leq |\Gamma(R)| < \infty$ implies that R is finite. Thus $\Gamma(R)$ is a finite graph (ie., has finitely many vertices) if and only if R is a finite ring or an integral domain. In particular, if $1 \leq |\Gamma(R)| < \infty$ it follows that R is finite and not a field.

Proof: If $1 \leq |\Gamma(R)|$, then there exist x and y in R, neither equal to zero, with $xy = 0$. Let $I = \mathrm{ann}(x)$. Then $y \varepsilon I$, and, in fact, $ry \varepsilon I$ for all $r \varepsilon R$. Suppose R is infinite with finitely many zero-divisors. Since I is a subset of the zero-divisors of R, it is finite. Thus, there exists an $i \varepsilon I$ such that $J = \{r \varepsilon R : ry = i\}$ is infinite. For $r, s \varepsilon J$, $(r - s)y = 0$. Thus, $\mathrm{ann}(y)$ is infinite, contradicting the fact that there are only finitely many zero-divisors. ■

II. Basic Structure

II.1 Connectivity

The class of graphs which are zero-divisor graphs of rings turns out to be fairly narrowly defined. They are connected graphs of small diameter and girth. Hence, zero-divisors may not be transitive, but in some sense, they are not all that far away from being transitive. We next demonstrate that the zero-divisor graphs, as we have defined them, are connected graphs of exceedingly small diameter and girth.

Theorem 8. Let R be a commutative ring (not necessarily finite). Then $\Gamma(R)$ is connected. Moreover, diam $\Gamma(R) \leq 3$.

<u>Proof:</u> Let $x, y \in \Gamma(R)$, with $x \neq y$. If $xy = 0$, then $d(x, y) = 1$. Suppose now that $xy \neq 0$. If $x^2 = 0 = y^2$, then $x - xy - y$ is a path of length two, and $d(x, y) = 2$. Suppose $x^2 = 0$ and $y^2 \neq 0$. There exists an element $b \in \Gamma(R)$ with $b \neq y$ such that $by = 0$. If $bx = 0$, then $x - b - y$ is a path of length two between x and y. If $bx \neq 0$, then $x - bx - y$ is a path of length two between x and y. In either case, $d(x, y) = 2$. A symmetric argument holds if $y^2 = 0$ and $x^2 \neq 0$. Thus we may suppose that neither x^2 nor y^2 is zero. Then there exist non-zero zero-divisors a , $b \in \Gamma(R)$ (not necessarily distinct) with $ax = 0 = by$. If $a = b$, then $x - a - y$ is a path of length 2, and hence

$d(x, y) = 2$. Thus we may assume $a \neq b$. Consider the element ab. If $ab = 0$, then $x - a - b - y$ is a path of length three, and hence $d(x, y) \leq 3$. If $ab \neq 0$, then $x - ab - y$ is a path of length two, and hence $d(x, y) = 2$. In all of the cases, there is a path between x and y of length less than or equal to three, and since x and y were arbitrary, it follows that the diameter of $\Gamma(R)$ is less than or equal to three. ■

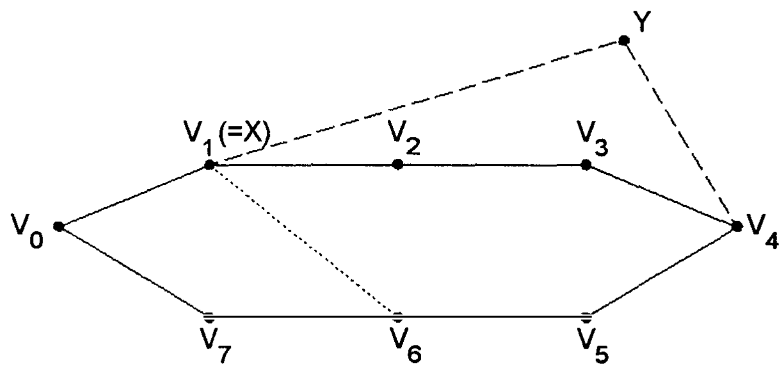
It is clear that $\mathbb{Z}_4$, $\mathbb{Z}_2 x \mathbb{Z}_2$, and $\mathbb{Z}_6$ have diameters zero, one, and two, respectively. Diameter three is also achieved. Consider the ring $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The distance between the elements $(1,1,0)$ and $(0,1,1)$ is three. In fact, a shortest path is $(1,1,0) - (0,0,1) - (1,0,0) - (0,1,1)$.

The fact that the distance between points is small also constrains the length of the shortest cycle, that is to say, the girth of the graph. The following corollary makes use of the previous theorem to establish a bound for the girth of a zero-divisor graph.

Corollary 9. If R is a ring, then the girth of $\Gamma(R)$ is less than eight.

Proof: It is enough to suppose to the contrary that we could find a ring R such that $\Gamma(R)$ has a smallest cycle, C, of length exactly eight, say,

$v_o - v_1 - v_2 - v_3 - v_4 - v_5 - v_6 - v_7 - v_8 = v_0$. Let P_1 denote the path $v_o - v_1 - v_2 - v_3 - v_4$, and P_2 denote the path $v_0 - v_7 - v_6 - v_5 - v_4$. To help in visualizing the proof, the figure below provides a hypothetical representation of each of the two main considerations which follow.



First, observe that for $0 < i < 4 < j < 8$, v_i and v_j are not connected. Assume the case is otherwise. Then $v_0 - \ldots - v_i - v_j - \ldots - v_0$ is a cycle of length less than eight contradicting the assumption that the girth is eight.. Now assume there is a path $v_o - x - y - v_4$ by the previous theorem. (If not, then there is a path $v_o - x - v_4$. The proof goes through if in this case we just identify x and y. The impossibility of v_o and v_4 being adjacent is apparent.) The fact just proved implies that the path $v_o - x - y - v_4$ intersects P_1, or perhaps P_2 , but not both. Thus, by symmetry we may as well assume that the path $v_o - x - y - v_4$ does not intersect P_2. This assumption yields a cycle $v_o - x - y - v_4 - v_5 - v_6 - v_7 - v_8 = v_0$ of length seven, the final contradiction. ■

Conjecture **10.** If R is any ring, then the girth of $\Gamma(R)$ is less than five.

There are rings whose zero-divisor graphs have girth exactly four, as we will demonstrate shortly. And in a later section, we demonstrate that the girth of the ring $\mathbf{Z}_N$, for any N, never exceeds four.

One should not interpret this, however, to mean that there cannot be cycles of length longer than seven in a given zero-divisor graph. In fact, the following corollary shows that there exist rings whose zero-divisor graphs admit cycles of arbitrarily specified length.

Example 11. Let T be an integral domain, and $n \geq 3$ an integer. Define R $= T[X_1, X_2, \ldots, X_n] / (X_1 X_2, X_2 X_3, \ldots, X_n X_1)$, and let $\mathbf{x}_i$ be the coset of X_i in R. Then $\mathbf{x}_1 - \mathbf{x}_2 - \ldots - \mathbf{x}_n - \mathbf{x}_1$ is a cycle of length n.

<u>Proof:</u> Note that $\mathbf{x}_i \mathbf{x}_j = 0$ if and only if $j = i + 1 \bmod n$. ∎

Although the cycles above have length n, they are by no means the shortest cycles in the graph, as the following proposition shows.

Proposition 12. If R is the ring in the previous example, with $n = 3$, or $n \geq 5$, then $\Gamma(R)$ contains a triangle. That is to say, the girth of $\Gamma(R)$ is three.

Proof: If $n = 3$, $\mathbf{x_1} - \mathbf{x_2} - \mathbf{x_3}$ is a triangle. If $n \geq 5$, then $\mathbf{x_1} - \mathbf{x_2 x_{n-1}} - \mathbf{x_n}$ is a triangle. ■

II.2 Rings with Prescribed Zero-Divisor Graphs

In this section, we consider certain small graphs to determine if they are the zero-divisor graphs for some ring. In fact, we note that as the number of vertices increases, the necessary complexity of the graphs make it impossible for many graphs to be zero-divisor graphs.

Proposition 13. Let $R = \mathbb{Z}_4$. Then $\Gamma(R)$ is a point.

Proof: The only vertex is the element **2.** ■

Proposition 14. Let $R = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then $\Gamma(R)$ consists of two vertices connected by an edge.

Proof: The vertices are $(1, 0)$ and $(0, 1)$. ■

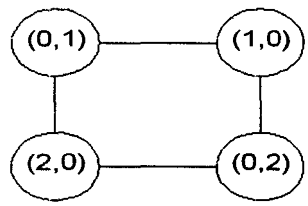
Proposition 15. Let $R = \mathbb{Z}_2[x, y] / (x^2, xy, y^2)$. Then $\Gamma(R)$ is a triangle. (This result is a special case of Proposition 21, which is to follow. Also, reference theorems 19 and 20.)

Proof: The non-zero zero-divisors of R are the cosets $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{x} + \mathbf{y}$. ■

This previous result is a special case of Proposition 16.

Proposition 16. Let $R = \mathbb{Z}_3 \times \mathbb{Z}_3$. Then $\Gamma(R)$ is a square.

Proof: The non-zero zero-divisors are (0, 1), (0, 2), (1, 0), and (2, 0). Thus $\Gamma(R)$ is:



■

Proposition 17. There is no ring R for which $\Gamma(R)$ is an n-gon for $n \geq 5$.

Proof: First consider the case $n = 5$. Suppose $z(R) = \{0, a, b, c, d, e\}$ with $0 = ab = bc = cd = de = ea$, and no other zero-divisor relations. Then $(-a)b = 0$ and $(-a)e = 0$. Thus $-a = a$. Similarly, $-x = x$ for all $x \in z(R)$. Also, $(b + e)a = 0$, so $b + e = 0$, a, b, or e. Clearly we cannot have $b + e = b$ or $b + e = e$, and $b + e = 0$ implies $b = -e = e$, which is a contradiction. Hence, $b + e = a$, and thus $a^2 = 0$. Similarly, $x^2 = 0$ for all $x \in z(R)$. Thus $z(R) = \mathrm{nil}(R) = \{0, a, b, c, d, e\}$, the unique prime ideal of R since R is finite. Hence $\mathrm{nil}(R) = \mathrm{ann}(x)$ for some non-zero $x \in z(R)$. But $|\mathrm{ann}(x)| = 4$ for every $0 \neq x \in z(R)$, a contradiction. The case for $n > 5$ is similar. ■

II.3 Ring-Theoretic Results

The discussion in the preceding section describes some of the types of graphs which may or may not occur. An interesting question is as follows: can a particular characterization of the zero-divisor graph of a ring tell us something about the ring itself, or vice-versa. The following theorem is a promising example in the affirmative.

Theorem 18. Let R be a finite ring which is not a field. Then there is a vertex of $\Gamma(R)$ which is adjacent to every other vertex if and only if either

i) $R \approx \mathbb{Z}_2 \times F$, where F is a finite field, or

ii) R is quasi-local.

<u>Proof:</u> ($\Leftarrow$) If $R \approx \mathbb{Z}_2 \times F$, then the element $(1, 0)$ is connected to every other vertex, since each has the form $(0, u)$, where u is non-zero. If R is quasi-local, then it must be the case that the ideal generated by Γ is in that unique maximal ideal. Since every maximal ideal is the annihilator of some element of R, that element annihilates Γ. Hence, the element is adjacent to every other element in Γ.

($\Rightarrow$) Assume that R is not quasi-local. Let $0 \neq a \varepsilon R$ be an element which is adjacent to every other element. Now a itself cannot be in $\text{ann}(a)$, for else R would be quasi-local, since in a finite ring, every element is either a zero divisor or a unit. Thus ann(a) is an ideal which is maximal among annihilators, and hence is prime by Proposition 4. Now if $a^2 \neq a$, then a^2 is a zero-divisor in ann(a). Thus $a^3 = 0$. Since ann(a) is prime, this implies that $a \in$ ann(a), a contradiction. Thus $a^2 = a$. That is, a is an idempotent. Hence $R = Ra \oplus R(1\text{-}a)$. Thus we can assume that $R \approx R_1 \times R_2$ and that (1, 0) is connected to all non-zero zero-divisors. If $1 \neq c \in R_1$, (c, 0) is a zero-divisor since (c, 0)(0, b)=0 for any $b \in R_2$. But this implies that (c, 0) = (c, 0)(1, 0) = 0, a contradiction unless c = 0. Hence, $R_1 \approx \mathbb{Z}_2$. If R_2 is not a field, then there is a non-zero nonunit $b \in R$. Then (1, b) must be a zero divisor, but this element cannot be connected to (1, 0). Thus R_2 must be a field. ■

Theorem 19. Suppose $\Gamma(R)$ is complete for a finite ring R. Then either,

i) $R \approx \mathbb{Z}_2 \times \mathbb{Z}_2$, or

ii) R is a quasi-local ring of characteristic p or p^2, and $|\Gamma(R)| = p^N - 1$, where p is a prime number, and $N \geq 1$.

<u>Proof:</u> For a field F, it is clear that $\Gamma(\mathbb{Z}_2 \times F)$ is not complete unless $F \approx \mathbb{Z}_2$. Otherwise, R must be quasi-local with maximal ideal, say, M, by the previous theorem. Now R cannot have composite characteristic: suppose p and q are distinct primes dividing characteristic R, with p < q. Then

$p^2 < pq$ implies that p^2 is a zero-divisor, but p and p^2 cannot be adjacent. Thus, the characteristic of R is p^n, for some $n \geq 1$. However, if $n \geq 3$, there is some number λ relatively prime to p such that $\lambda p < p^n$, so that p and λp are non-adjacent zero-divisors. (For $p=2$, put $\lambda=3$. If $p>2$, put $\lambda=2$.) Thus the characteristic of R is p or p^2. Thus, each element of M has additive order $1, p$, or p^2. Hence, as an abelian group, $M \approx (\oplus \mathbb{Z}_p) \oplus (\oplus \mathbb{Z}_{p2})$, so that $|M| = p^N$ for some $N \geq 1$. It follows that $|\Gamma(R)| = p^N - 1$. ■

Theorem 20. The graph $\Gamma(R)$ is complete *if and only if* either

(1) $R \approx \mathbb{Z}_2 \times \mathbb{Z}_2$, or

(2) $xy = 0$ for every $x, y \in z(R)$.

To put the forward (and most interesting) direction in other words, if $\Gamma(R)$ is complete then the zero-divisors of R are nilpotent of order two, except in the case $R \approx \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof: The *if* direction is completely clear (pun intended). For the *only if* direction, suppose that (2) fails. Then there is an $0 \neq x \in z(R)$ with $x^2 \neq 0$. We show that $x^2 = x$, which will imply (1). Suppose to the contrary that $x^2 \neq x$. Then $x^3 = x^2x = 0$. Hence, $x^2(x + x^2) = 0$ with $x^2 \neq 0$, so $x + x^2 \in z(R)$. If $x + x^2 = x$, then $x^2 = 0$, a contradiction. Thus the fact that $x + x^2$ and x are zero-divisors of R, together with the fact that $x + x^2 \neq x$ implies that

$x^2 = x^2 + x^3 = x(x + x^2) = 0$, another contradiction. Hence, we must have $x^2 = x$, as claimed. Thus, $R = Rx \oplus R(1-x) \approx R_1 \oplus R_2$. Let $1 \neq a \in R_1$. Then $(a, 0) \in z(R)$ and $(1, 0) \in z(R)$, so $0 = (a, 0)(1, 0) = (a, 0)$ which implies that $a=0$. Thus $R_1 \approx \mathbb{Z}_2$. Similarly $R_2 \approx \mathbb{Z}_2$, and so $R \approx \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

More, in fact, can be shown. We demonstrate that for each prime p and integer $n \geq 1$, there is a ring R with $\Gamma(R)$ complete of order $p^n - 1$.

Proposition 21. Let T be an integral domain and $R = T[X_1, X_2, \ldots, X_n] / $ (all degree 2 monomials). Then $\Gamma(R)$ is complete on $|T|^n - 1$ vertices. In particular, if $T = \mathbb{Z}_p$, then $|\Gamma(R)| = p^n - 1$.

Proof: We may write $R = \{a_0 + a_1\mathbf{x}_1 + \ldots + a_n\mathbf{x}_n \mid a_i \in T\}$. Then $z(R)$ is that subset of R, where $a_0 = 0$. Hence, the product of any two distinct zero-divisors is zero, since each term in the product has degree two. It is clear that $|\Gamma(R)| = |T|^n - 1$. ■

We give another example:

Example 22. If p is a prime number, then $\Gamma(\mathbb{Z}_{p^2})$ is complete.

Proof: Each zero-divisor is divisible by p. Hence, the product of any two zero-divisors is zero. ■

Note that $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p[X]/(X^2)$ are not isomorphic as rings, but we have $\Gamma(\mathbb{Z}_{p^2}) = \Gamma(\mathbb{Z}_p[X]/(X^2)) = K_{p-1}$, the complete graph on $p-1$ vertices.

III. Beck's Theorem and $\Gamma(\mathbb{Z}_N)$

III.1 Colorings

In discussing the problem of coloring the zero-divisor graph, Beck [3] chooses as an example the graph of $\mathbb{Z}_N$. In doing so, he proves the following interesting theorem which we will exploit to prove some specific results regarding colorings of $\Gamma(\mathbb{Z}_N)$. In the next section, we make further characterizations of the structure of $\Gamma(\mathbb{Z}_N)$.

Definition 23. A ***coloring*** of a graph is an assignment of colors to the vertices of a graph in a way such that no two adjacent vertices receive the same color. The minimal number of colors needed to color a graph Γ is denoted by $\chi(\Gamma)$, and called chromatic number.

Theorem 24. (Beck) Let $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots q_r$ be distinct prime numbers and let $N = p_1^{2n_1} p_2^{2n_2} \ldots p_k^{2n_k} q_1^{2m_1+1} q_2^{2m_2+1} \ldots q_r^{2m_r+1}$. Then

$$\chi({}_0\Gamma(\mathbb{Z}_N)) = cl({}_0\Gamma(\mathbb{Z}_N)) = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} q_1^{m_1} q_2^{m_2} \ldots q_r^{m_r} + r.$$

Proof: Let $y_0 = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} q_1^{m_1+1} q_2^{m_2+1} \ldots q_r^{m_r+1}$. Then $y_0^2 = 0$ in $\mathbb{Z}_N$ and thus $y_0\mathbb{Z}_N$ is a clique with $p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} q_1^{m_1} q_2^{m_2} \ldots q_r^{m_r}$ elements. Put $y_i = y_0 / q_i$, where $1 \leq i \leq r$. The set $c = y_0\mathbb{Z}_N \cup \{y_1, y_2, \ldots, y_r\}$ is a clique containing $t = p_1^{n_1}\ p_2^{n_2} \ldots p_k^{n_k}\ q_1^{m_1}\ q_2^{m_2} \ldots\ q_r^{m_r} + r$ elements. Hence $cl(\mathbb{Z}_N) \geq t$. In order to show that $cl(\mathbb{Z}_N) \leq t$, we first attach a distinct color to each of the elements in the clique C. Furthermore, let $x_i = N / p_i^n$, with $1 \leq i \leq k$. We note that $x_1, \ldots, x_k$ belong to C and hence have been equipped with a color. Let $f(y)$ denote the color of an element y and color the remaining elements of $\mathbb{Z}_N$ as follows: Pick x not in $y_0\mathbb{Z}_N$. If $p_1^{n_1}\ p_2^{n_2} \ldots p_k^{n_k}$ divides x define $f(x) = f(y_j)$ where $j = \min\{i : q_i^{m\ +1}$ fails to divide $x\}$. If $p_1^{n_1}\ p_2^{n_2} \ldots p_k^{n_k}$ does not divide x, let $f(x) = f(x_j)$, where $j = \min\{i : p_i^n$ fails to divide $x\}$. It is easily seen that this coloring attaches different colors to adjacent vertices. ■

Proposition 25. For every positive integer M, there is an N with $\chi({}_o\Gamma(\mathbb{Z}_N)) = cl({}_o\Gamma(\mathbb{Z}_N)) = M$.

<u>Proof:</u> Let $N = p_1\, p_2 \ldots p_{M-1}$, where p_i is the i^{th} prime, and apply Beck's theorem. ■

It should be noted that this N is not minimal with respect to the proposition. For example, consider $M = 7$ and let $N = 3^2\, 2^{2\bullet 1\ +1} = 72$. By Beck's theorem, the calculation $3\bullet 2 + 1 = 7$ implies that the graph $\Gamma(\mathbb{Z}_{72})$ may be colored with only seven colors, while the proof of the above theorem would have N be $2\bullet 3\bullet 5\bullet 7\bullet 11\bullet 13 = 30{,}030$.

III.2 The Zero-Divisor Graphs of $\Gamma(\mathbb{Z}_N)$

In addition to these particular coloring results, we can provide more specific characterizations of the structure of $\Gamma(\mathbb{Z}_N)$. We will make use of the following graph-theoretic definition.

Definition 26. A graph whose vertices may be partitioned into sets V_1 and V_2 in such a way that no two vertices in the same vertex set are connected is called a ***bipartite graph***. A ***complete bipartite graph*** is a bipartite graph which is maximal with respect to the number of edges.

Note that a bipartite graph *cannot admit a triangle* as a subgraph, for else two vertices in the same vertex class would necessarily be connected.
One can see that the girth of a bipartite graph, if it is defined, must be an even number greater than or equal to four. Figure 2 below shows the complete bipartite graph for the zero-divisor graph of the ring $\mathbb{Z}_{20}$.

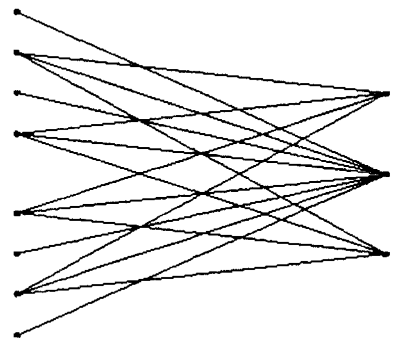


Figure 2: The Zero-Divisor Graph of $\mathbb{Z}_{20}$

Proposition 27. $\Gamma(\mathbb{Z}_N)$ is triangle-free if and only if, either $N = pq$ for p and q distinct primes, or $N = 2^2p$ for p a prime, or $N = 3^2$, or $N = 2^2$, or when N is a prime.

Proof: It is necessary to treat several cases separately. The basic approach in each of the following cases is to find 3 *distinct* mutually adjacent vertices.

Case a: N is divisible by at least three distinct primes, say p , q and r. Then $\mathbf{prN/q}$, $\mathbf{qpN/r}$ **and** $\mathbf{qrN/p}$ are pairwise adjacent, nonzero distinct elements of $\mathbb{Z}_N$. Thus $\mathbf{prN/q - qpN/r - qrN/p}$ is a triangle.

Case b: N is divisible by the squares of two distinct primes, say p and q. Let $d = N / p^2q^2$. Then $\mathbf{pq^2d - p^2qd - pqd}$ is a triangle.

Case c: $p \geq 5$ and p^2 divides N. Let $d = N / p^2$. Then $p \geq 5$ implies that $p^2 d > 3pd$, which in turn implies that $0 < pd < 2pd < 3pd < N$. It follows that **pd - 2pd - 3pd** is a triangle.

Case d: $N = 2^n$, where $n \geq 4$. Then $\mathbf{2^{n-2} - 3 \bullet 2^2 - 2^{n-1}}$ is a triangle. This is because $n \geq 4$ implies that $3 \bullet 2^2 < 2^n$.

Case e: $N = 3^n$, where $n \geq 3$. Then $\mathbf{3^{n-2} - 2 \bullet 3^2 - 3^{n-1}}$ is a triangle. This is because $n \geq 3$ implies that $2 \bullet 3^2 < 3^{n-1}$.

Case f: $N = 3^2 p$, where p is any prime. Then **3 - 3p - 3(2p)** is a triangle. This is because $3(2p) < 3^2 p$.

Case g: $N = 2^n p$, where p is any prime, and $n \geq 3$. Then $\mathbf{2^{n-1} - 2p - 2^{n-1}p}$ is a triangle.

This leaves the rings listed in the statement of the theorem as the only remaining possibilities for admitting triangle-free graphs. Two of the cases require argument.

Claim 1) If $N = 2^2q$, where q is any odd prime, then $\Gamma(\mathbb{Z}_N)$ is triangle-free. To see this, let $U = \{\lambda 2 \in \Gamma(\mathbb{Z}_N) : (\lambda, q) = 1\} = \{\lambda 2 \in \Gamma(\mathbb{Z}_N) : \lambda \neq q\}$ and $V = \{\lambda q : \lambda q < N\} = \{q, 2q, 3q\}$. Since q does not divide any element of U, none of the elements of U are adjacent. And since no element in V is divisible by 2 other than $2q$, no elements of V are adjacent. The sets U and V partition the vertices of $\Gamma(\mathbb{Z}_N)$, and it follows that the graph is bipartite and hence is triangle-free.

Claim 2) If $N = pq$, where p and q are distinct primes, then we partition the vertices into sets $U = \{\lambda p \in \Gamma(\mathbb{Z}_N) : (\lambda, q)=1\}$ and $V = \{\lambda q \in \Gamma(\mathbb{Z}_N) : (\lambda,p)=1\}$. It is clear that this partition shows that $\Gamma(\mathbb{Z}_N)$ is bipartite. Furthermore, notice that $xy = 0$ for every $x \in U$ and $y \in V$. Hence, $\Gamma(\mathbb{Z}_N)$ is a complete bipartite graph. ■

Theorem 28. diam $\Gamma(\mathbb{Z}_N) \in \{0, 1, 2, 3\}$.

<u>Proof:</u> The table at the end of this section gives several examples of the cases 0, 1 and 2, and in each the reasoning is straightfoward. A few words regarding the case $\Gamma(\mathbb{Z}_N) = 3$ may be useful. If $N = 2^np$, where p is a prime number, then $d(2, p) = 3$, since the vertex **2** is connected only to **2p**, which is not connected to **p**. The vertex **2p** is connected to only to vertices divisible by **4**, any of which are in turn connected to the vertex **p**. ■

Theorem 29. Girth($\Gamma(\mathbf{Z}_N)$) ε {3, 4} or is undefined.

<u>Proof:</u> If $\Gamma(\mathbf{Z}_N)$ has a triangle, then its girth is three. Otherwise, N must be characterized by one of the possibilities in the theorem above. By inspection of the triangle-free cases above, the girth is equal to four, or is undefined. (Set p=3 and q=5 in the above example to see an example where the girth is four.) ■

N	No. Vertices	No. Edges	Diameter	Girth	Remarks
p	0	0	0	undefined	$\Gamma(\mathbb{Z}_p) = \varnothing$
2^2	1	0	0	undefined	
3^2	2	1	1	undefined	
p^2 ($p \geq 5$)	p-1	$\binom{p-1}{2}$	1	3	complete graph K_{p-1}
2^3	3	2	2	undefined	
p^n ($n \geq 3$)	$p^{n-1} - 1$	$\sum (p-1)^{\lfloor i/2 \rfloor}$	2	3	quasi-local: $\mathbf{p^{n-1}}$ is attached to everything
2^2p $p \geq 3$	2p + 1	4p - 4	3	4	bipartite graph (but not complete)
pq	q-1 + p-1	(q-1)(p-1)	2	4	complete bipartite graph $K_{q-1,p-1}$
all others			2	3	

$\Gamma(\mathbb{Z}_N)$ Summary Table: (p, q distinct primes)

IV. The Automorphism Group of $\Gamma(\mathbb{Z}_N)$

A useful measure of symmetry in the graph $\Gamma(R)$ is its automorphism group.

Definition 30. A ***automorphism*** of a graph Γ is a permutation ϕ of the vertices of the graph which preserves adjacency between points. More precisely, (x, y) is an edge of Γ if and only if $(\phi(x), \phi(y))$ is also an edge of Γ. This set of automorphisms forms a group under composition. We call this group ***the automorphism group*** of Γ, and denote it $\textit{Aut}\ \Gamma$.

One might say that a lack of symmetry in a graph is associated with a trivial automorphism group, or perhaps an automorphism group which is small in relation to the total number of vertices in the graph. The converse is evidently true for zero-divisor graphs of rings, at least as evidenced by the following theorem.

Theorem 31. The automorphism group of $\Gamma(\mathbb{Z}_n)$ is a direct product of symmetric groups.

Proof: For each d dividing n, with $1 < d < n$, let $V_d = \{ \lambda d \in \mathbb{Z}_n \mid (\lambda, n) = 1\}$. Let V denote the vertices of $\Gamma(\mathbb{Z}_n)$. Then V is the disjoint union of the V_d's.

Let $x,\ y \varepsilon V_d$ for some $d \mid n$, with $x \neq y$. By the Fundamental Theorem of Arithmetic, $ax = 0$ *if and only if* $ay = 0$, since the only common divisor of n that x and y share is d itself. (Observe that $ax = 0$ if and only if $ad = 0$, since $\lambda \varepsilon U(\mathbb{Z}_n)$.) Thus, the *if* direction implies that the transposition (x, y) induces an automorphisms of $\Gamma(\mathbb{Z}_n)$ (by fixing all other vertices). The collection of these transpositions as x and y vary over V_d then generate a symmetric group of cardinality $|V_d|$ acting on $\Gamma(\mathbb{Z}_n)$. The *only if* direction implies that the orbit of any fixed $x \varepsilon V_d$ is restricted to V_d. Specifically, if $\theta \varepsilon \mathrm{Aut}(\Gamma(\mathbb{Z}_n))$, then the map $\mathrm{Aut}(\Gamma(\mathbb{Z}_n)) \rightarrow \Pi\, S_{k(d)}$ given by $\theta \rightarrow \theta|_{V_d}$, where $k(d) = |V_d|$ and the product ranges over all $d \mid n$ with $1 < d < n$, is an isomorphism. ■

The explicit characterization of the automorphism group of $\Gamma(\mathbb{Z}_n)$ just given is worth restating separately. Recall the definition of V_d in the proof above: for $d | n$ we define $V_d = \{ \lambda d \varepsilon \mathbb{Z}_n \mid (\lambda, n) = 1\}$.

Theorem 32. $\mathrm{Aut}(\Gamma(\mathbb{Z}_n)) \approx \Pi\, S_{|V_d|}$, where the product ranges over all $d | n$ and $1 < d < n$.

Example 33. Consider the ring $R = \mathbb{Z}_{12}$. The automorphism group of $\Gamma(\mathbb{Z}_{12})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. This is not hard to see combinatorially.

By examining the degrees of the vertices, we see that the orbits indicated in Figure 3 below are the only possible ones. To be precise, let us use the notation in the proof of the main theorem (31) in this section: we have $V_2 = \{2, 10\}$, $V_3 = \{3, 9\}$, $V_4 = \{4, 8\}$, and $V_6 = \{6\}$. (Note that if $1 < d < 12$, then $d \mid 12 \Leftrightarrow d = 2, 3, 4$ or 6.) The elementary abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is the only one which is the product of three disjoint involutions.

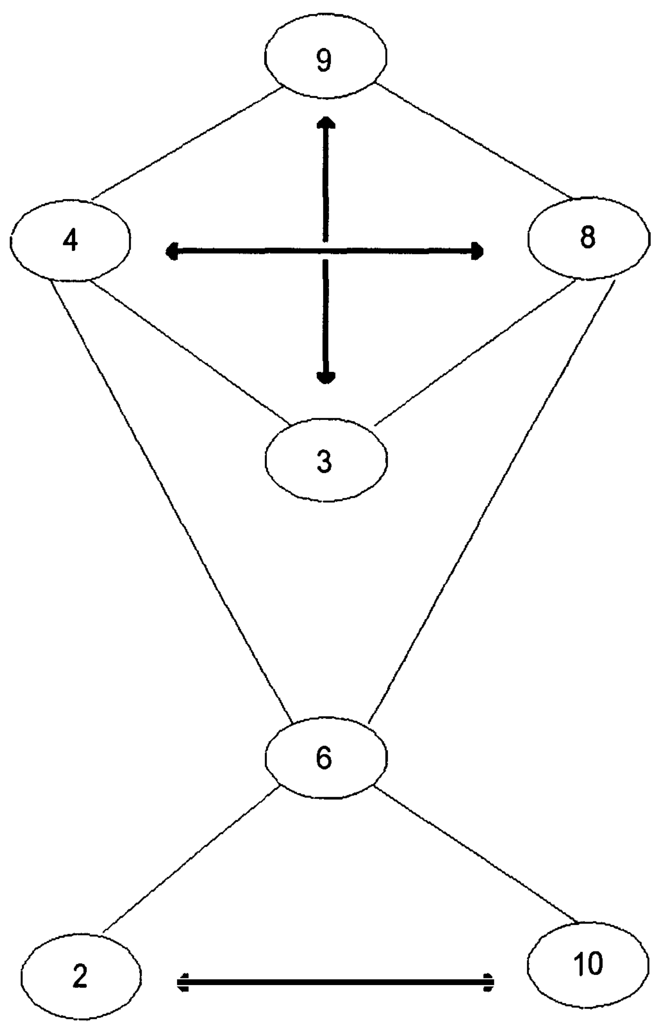


Figure 3: The Orbits of the Automorphism Group of $\Gamma(\mathbb{Z}_{12})$

V. Conclusion

Why look at colorings, or at zero-divisor graphs in the first place? One obvious answer is that the graphs are highly connected and exhibit considerable symmetry. In these cases, colorings provide some insight into the degree to which both are present. The zero-divisor graph seems to extract certain essential information relative to zero-divisors. In particular, it provides some clarity as to the "non-transitivity" of the zero-divisor relation. Theorem 18 suggests that an understanding of the zero-divisors of a ring by themselves provides crucial information about the whole ring. The extent to which this relationship can be exploited needs further investigation. Furthermore, graphs could be associated with rings in ways other than with the zero-divisor relation. For example, one could associate a graph with a ring in the following way: let I be an ideal of a ring R. Then the vertices of the graph could be the elements of the ring, and two elements are related by an edge if their product were an element of the ideal I. Another interesting possibility is to consider the zero-divisor graph of a non-commutative ring. In such rings, the relation $xy = 0$ does not necessarily imply the relation $yx = 0$, and hence we would require the use of directed graphs which do not require symmetric edge relations.

REFERENCES

REFERENCES

[1] D.D. Anderson and M. Naser, Beck's Coloring of a Commutative Ring, *Journal of Algebra* **159** (1993), 500-514.

[2] M. Aschbacher, "Finite Group Theory," Cambridge University Press, Cambridge, 1972.

[3] I. Beck, Coloring of commutative rings, *Journal of Algebra* **116** (1988), 208-226.

[4] F. Harary, "Graph Theory," Addison-Wesley, Reading, MA, 1972.

[5] I. Kaplansky, "Commutative Ring Theory," Revised Edition, University of Chicago Press, 1974.

VITA

Philip Stephen Livingston was born in Oak Ridge, Tennessee on June 16, 1958. He attended Powell Elementary and Powell High School. He attended the University of Tennessee from the summer of 1976 until the spring of 1979, when he began work in the computer industry. Mr. Livingston graduated cum laude with a bachelor of Arts degree in Mathematics from the University of Maryland, College Park, in May 1984. He continued to work in all aspects of the computer industry including several years of management. In January of 1992 he returned to the University of Tennessee to pursue an advanced degree in mathematics. Presently, he enjoys research in Commutative Ring Theory and a continuing instructorship at the University of Tennessee.