UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

OSAMA SHAFAH

KONAČNI PRSTENI I USMERENI GRAFOVI: JEDNA NEOBIČNA VEZA

DOKTORSKA DISERTACIJA

BEOGRAD, 2013

UNIVERSITY OF BELGRADE
FACULTY OF MATHEMATICS

OSAMA SHAFAH

AN INTERESTING RELATIONSHIP BETWEEN FINITE RINGS AND GRAPHS

DOCTORAL THESIS

BEOGRAD, 2013

Acknowledgements

First and foremost I want to thank my supervisor Dr. A. Lipkovski, I would like to thank him for his continuous support. This thesis would not have been possible without his enthusiastic approach, help and kind encouragement.

Besides my supervisor, I would like to thank the rest of my thesis committee: Dr. Žarko Mijajlović and Dr. Zoran Petrović, for their encouragement, insightful comments.

My gratitude is also expressed to my family and friends for their full support, patience and understanding.

Podaci o mentoru i članovima komisije:

MENTOR:
redovni profesor dr Aleksandar Lipkovski
Matematički fakultet,
Univerzitet u Beogradu

_____

ČLANOVI KOMISIJE :
redovni profesor dr Žarko Mijajlović
Matematički fakultet,
Univerzitet u Beogradu

_____

vanredni profesor dr Zoran Petrović
Matematički fakultet,
Univerzitet u Beogradu

_____

Datum odbrane:

Contents

Introduction

In this thesis we will give an interesting relation between finite rings and their graphs, such relations are obtained in following way.

Consider a directed graph $G = G(\mathbb{Z}_n) = (V, E, \emptyset)$ on a finite ring $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, where V, E are sets of vertices and edges respectively, and $\emptyset: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ defined by $\emptyset(a, b) = (a + b, ab)$. Since R is finite, it has an integer characteristic $n = char\ R \in \mathbb{N}$. If n is not a prime, then R has zero divisors and $R[X]$ is not a unique factorization ring, but if it is prime, then R nevertheless could have zero-divisors (e.g., $\mathbb{Z}_2 \times \mathbb{Z}_2$). Let m and k be relatively prime numbers, such that $n = mk$, $m < k$ and define two maps

$$h_1: \mathbb{Z}_n \to \mathbb{Z}_m,$$

$$h_2: \mathbb{Z}_n \to \mathbb{Z}_k$$

by $h_1(a) = (a\ mod\ m)$ and $h_2(a) = (a\ mod\ k)$ respectively, so h_1 and h_2 are homomorphism maps, suppose that $\vec{C}_s = 012 \ldots s-1$ is a directed cycle of length s in a directed graph G, then many interesting algebraic relations will exist between longest cycles in $\mathbb{Z}_n$, $\mathbb{Z}_m$ and $\mathbb{Z}_k$, which will be shown up in the chapter III.

Scientific field (naučna oblast): Mathematics (matematika)
Narrow scientific field (uža naučna oblast): Abstract Algebra (Izvod Algebra)
UDC: 512.552.4:519.17(043.3)

Chapter I

Preliminaries

This first chapter introduces the fundamental definitions and properties of rings and graphs. We will start with a ring theory and throughout this paper, R denotes a finite commutative ring with unity.

(I) RINGS

In this section, we assume that a ring R is an abelian group with a multiplication operation $(a, b) \to ab$, which is associative, and satisfies the distributive laws $a(b + c) = ab + ab, (a + b)c = ac + bc$.

1.1 General ring axioms

1.1.1 Definition

A ring $(R, +, \cdot)$ is said to be commutative if $a \cdot b = b \cdot a$ for all $a, b \in R$.

1.1.2 Definition

A ring $(R, +, \cdot)$ is said to be ring with unity if there exist element $e \in R$ such that $a \cdot e = a$ for all $a \in R$. The element e is called the unity of R.

The unity is also called the identity or unit element of R. Generally it is denoted by 1 (not to be confused with the integer 1). The unity of a ring, if it exists, is unique.

1.1.3 Example

The set of integers $\mathbb{Z}$ under the usual addition and multiplication is a commutative ring with unity.

1.1.4 Example

$2\mathbb{Z}$, under the usual addition and multiplication is a commutative ring without unity.

1.1.5 Example

Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Under the usual addition and multiplication of numbers, $\mathbb{Z}[\sqrt{2}]$ is a commutative ring with unity.

1.1.6 Definition

The ideal I is an additive subgroup of a ring R, which satisfies the condition:

$$ar \in I \text{ for all } a \in I, \text{ and all } r \in R.$$

We say that an ideal I of R is proper if neither $I = \{0\}$ nor $I = R$.

1.1.7 Example

$(2\mathbb{Z}, +, \cdot)$ is a proper ideal in $(\mathbb{Z}, +, \cdot)$.

1.1.8 Definition

Let R and S be rings. A map $f: R \to S$ is called a ring homomorphism if $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in R$. If R and S are rings with identity, it's customary to also require that $f(1_R) = 1_S$ [usually we just write $f(1) = 1$]. If f is also a bijection then it is called an isomorphism and we say that R and S are isomorphic rings, and we write $R \cong S$.

1.1.9 Definition

If $f: R \to S$ is a ring homomorphism, we define the *kernel* of f in the most natural way:

$Kerf = \{r \in R, f(r) = 0\}$.

Since a ring homomorphism is in particular a group homomorphism, we already know that f is injective if and only if $Kerf = \{0\}$. If $f \neq 0$, it is easy to check that $Kerf$ is a proper ideal.

1.1.10 Example

The function $f: \mathbb{Z} \to \mathbb{Z}_n$, defined by $f(a) = \bar{a} = a \ mod \ n$ is a surjective ring homomorphism with *kernel* nZ. [There is no ring homomorphism $\mathbb{Z}_n \to \mathbb{Z}$ for n > 1 except the 0 –homomorphism].

1.1.11 Lemma

Suppose $f: R \to S$ is a ring homomorphism and the only ideals of R are $\{0\}$ and R. Then f is injective.

1.1.12 Definition

Let R and S be rings. The product ring $R \times S$ of R and S is the set consisting of all ordered pairs (r, s), where $r \in R$ and $s \in S$. Addition and multiplication are defined component-wise: For $r_1, r_2 \in R$ and $s_1, s_2 \in S$,

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2).$$

$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2).$$

I won't go through the verification of all the axioms; basically, everything works because everything works in each component separately.

1.1.13 Example

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

It is not difficult to prove that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

1.2 Quotient rings

Let I be a proper ideal of R. Since I is an additive subgroup of R by definition, it makes sense to speak of cosets $r + I$ of $I, r \in R$. Furthermore, a ring has a structure of abelian group for addition, so I satisfies the definition of a normal subgroup. From group theory, we thus know that it makes sense to speak of the quotient group:

$R/I = \{r + I, r \in R\}$.

1.2.1 Definition

The set of cosets of an ideal I given by $R/I = \{r + I, r \in R\}$ is a ring with identity $1_R + I$ and zero element $0_R + I$ called a quotient ring.

Note that we need the assumption that I is a proper ideal of R to claim that R/I contains both an identity and a zero element (if $R = I$, then R/I has only one element).

1.2.2 Example

Consider the ring of matrices $M_2(\mathbb{Z}_2[i])$, where $\mathbb{Z}_2$ denotes the integers modulo 2, and $i^2 = -1 \equiv 1 \, mod \, 2$. This is the ring of 2×2 matrices with coefficients in $\mathbb{Z}_2[i] = \{a + ib, a, b \in \{0,1\}\}$. Let I be the subset of matrices with coefficients taking values 0 and $1 + i$ only. It is an ideal of $M_2(\mathbb{Z}_2[i])$. Indeed, take a matrix $U \in I$, a

matrix $M \in M_2(\mathbb{Z}_2[i])$, and compute UM. An immediate computation shows that all coefficients are of the form $a(1+i)$ with $a \in \mathbb{Z}_2[i]$, that is all coefficients are in $\{0, 1+i\}$. Clearly I is an additive group. We then have a quotient ring $M_2(\mathbb{Z}_2[i])/I$.

We have seen that $Kerf$ is a proper ideal when f is a ring homomorphism. We now prove the converse.

1.2.3 Proposition

Every proper ideal I is the *kernel* of a ring homomorphism.

1.2.4 Definition

An element x of a ring R is called nilpotent if there exists some positive integer n such that $x^n = 0$.

1.2.5 Example

In the ring $\mathbb{Z}/9\mathbb{Z}$, the equivalence class of 3 is nilpotent because 3^2 is congruent to 0 modulo 9.

1.3 Maximal and prime ideals

Here are a few special ideals.

1.3.1 Definition

Let R be a ring. The ideal $\{ra: r \in R\}$ is called the principal ideal generated by $a \in R$

and is denoted by $< a >$. An ideal I is called principal if there exists $a \in R$ such that $I =< a >$.

1.3.2 Theorem

Let A be any subset of a ring R, and let $\{I_\gamma\}_{\gamma \in \Gamma}$ be the family of all ideals in R such that $A \subseteq I_\gamma$. Then $I = \bigcap_{\gamma \in \Gamma} I_\gamma$ is the smallest ideal in R containing A, and we write $I =< A >$.

1.3.3 Definition

A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

1.3.4 Example

The ideal $3\mathbb{Z}$ is maximal in $\mathbb{Z}$, but the ideal $4\mathbb{Z}$ is not since $4\mathbb{Z} \subseteq 2\mathbb{Z} \subseteq \mathbb{Z}$.

1.3.5 Definition

Ideals I and J are called comaximal or relatively prime if $I + J = R$.

One can prove that every proper ideal is contained in a maximal ideal, and that consequently every ring has at least one maximal ideal. But we will skip that since it is not in our concentration. Let us mention the following theorem, which will be used for characterizing maximal ideals.

1.3.6 Theorem

If I is an ideal of a ring R, then the canonical map

$$\pi: R \to R/I$$

sets up a one-to-one correspondence between

• the set of all subrings of R containing I and the set of all subrings of R/I,

• the set of all ideals of R containing I and the set of all ideals of R/I. ■

Here is a characterization of maximal ideals in commutative rings [Our assumptionn is that, the reader knows definitions of a field and an integral domain].

1.3.7 Theorem

Let M be an ideal in a ring R. Then M is a maximal if and only if R/M is a field.

1.3.8 Definition

A prime ideal in a commutative ring R is a proper ideal P of R such that for any $a, b \in R$, we have that:
$ab \in P$ if and only if $a \in P$ *or* $b \in P$.

1.3.9 Example

The ideal $< 6 >$ is not a prime ideal in $\mathbb{Z}$, since $2 \times 3 \in < 6 >$ although neither 2 nor 3 belong to $< 6 >$. However the ideal $< 5 >$ is prime in $\mathbb{Z}$, since the product of two integers is a multiple of 5 only if at least one of the two is a multiple of 5.
The prime ideals of $\mathbb{Z}$ are precisely the maximal ideals; they have the form $< p >$ for a prime p, and the zero ideal $< 0 >$ (which is not proper).

Here is again a characterization of a prime ideal P of R in terms of its quotient ring R/P.

1.3.10 Theorem

Suppose that P is an ideal in R. Then P is a prime ideal if and only if R/P is an integral domain.

1.3.11 Corollary

In a commutative ring, a maximal ideal is prime.

In the following we are giving some definitions which will be used in the next chapter.

1.3.12 Definition

Let R be a commutative ring with identity. Let $J(R)$ be the intersection of all maximal ideals of R. $J(R)$ is called the Jacobson radical of R.

1.3.13 Definition

Let R be a commutative ring with identity. Let $N(R)$ be the intersection of all prime ideals of R. Then $N(R)$ is called the nilradical of R. If $N(R) = \{0\}$, then R is called a reduced ring.

1.3.14 Definition

Let R be a ring, and let M be a left R-module. Choose a nonempty subset S of M. The annihilator, denoted by $ann_R(S)$, is the set of all elements r in R such that for each s in S, $rs = 0$. [In set notation, $ann_R(S) = \{r \in R: for\ all\ s \in S, rs = 0\}$].
The annihilator of a single element x is usually written $ann_R(x)$ instead of $ann_R(\{x\})$.
If the ring R can be understood from the context, the subscript R can be omitted.

1.4 Fermat's Little Theorem

In what follows Fermat's Little Theorem will be used so we state it for completeness. Despite its name, Fermat's Little Theorem is one of most important theorems. It was presented by Pierre de Fermat's in 1640 without proof in one of his letters. Leonhard Euler provided the first published proof in 1736. The theorem is very useful as a way of testing very large primes.

1.4.1 Proposition

Let R be a finite commutative ring and e be the identity element of R. Then $x^{|R|} = e$ for all $x \in R$.

Proof

Suppose R is a finite commutative ring, define $\pi_x: R \to R$ by $\pi_x(r) = xr$ for all $r \in R$, so π_x is a bijective map (multiplying by x^{-1} is the inverse map). Hence

$\prod_{r\in R} r = \prod_{r\in R} xr = x^{|R|} \prod_{r\in R} R,$

and this implies $x^{|R|} = e$.

1.4.2 Theorem (Fermat's Little Theorem)

Let p be a prime number and $a \in \mathbb{Z}$ be a number that is prime to p. Then

$a^{p-1} \equiv 1 \, mod \, p.$

Proof. See in [11, p. 298].

1.4.3 Example

from the last theorem, then we know that:

$(47)^2 \equiv 1 \, mod \, 3.$

$(110)^6 \equiv 1 \, mod \, 7.$

(II) GRAPHS

Many real-world situations can conveniently be described by means of a diagram consisting of a set of points together with edges joining certain pairs of these points. For example, the points could represent people, with edges joining pairs of friends; or the points might be communication centers, with edges representing communication links. Notice that in such diagrams one is mainly interested in whether or not two given points are joined by an edge; the manner in which they are joined is immaterial.

A mathematical abstraction of situations of this type gives rise to the concept of a graph.

1.5 General definitions and axioms

1.5.1 Definition

A graph G is an ordered triple (V, E, Φ) consisting of a non-empty set V of vertices (points-nodes), a set E of edges disjoint from V, and an incidence map Φ that

associates with each edge of G an ordered or unordered pair of (not necessarily distinct) vertices of G.

If e is an edge and u , v are vertices such that $\Phi(e) = uv$, then e is said to join u and v; the vertices u and v are called the ends of e.

We shall assume throughout this work that both sets $V$and E of a graph are finite. It would be convenient to write a graph $G = (V, E, \Phi)$ as $G = (V, E)$ or simply as G.

The following example of graph should serve to clarify the definition.

1.5.2 Example

Let $G = (V, E, \Phi)$. Where $V = \{v_1, v_2, v_3, v_4, v_5\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and Φ is defined by :

$\Phi(e_1) = v_2v_1$, $\Phi(e_2) = v_2v_3$, $\Phi(e_3) = v_3v_3$, $\Phi(e_4) = v_3v_4$,$\Phi(e_5) = v_2v_4$, $\Phi(e_6) = v_4v_5$, $\Phi(e_7) = v_2v_5$, and $\Phi(e_8) = v_2v_5$.Then G is the graph which is presented in the following diagram

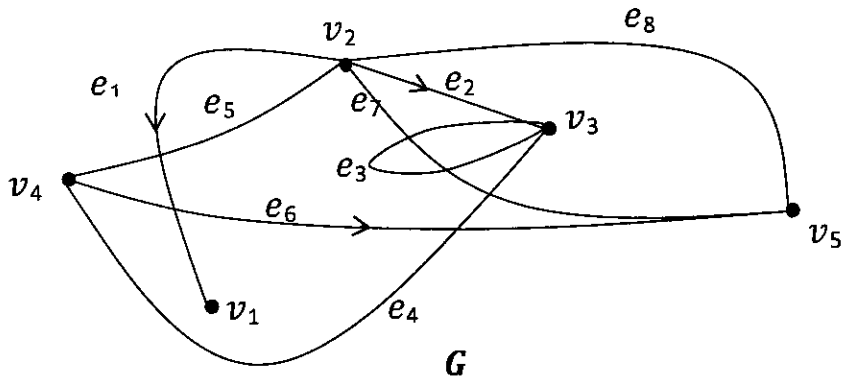


Figure 1.5.1 A diagram of the graph G.

Notice that the definition of a graph implies that to every edge of the graph G we can associate an ordered or unordered pair of nodes (vertices) of the graph. If an edge $e \in E$ is thus associated with an ordered pair $< u, v >$ or an unordered pair (u, v) where $u, v \in E$, then we say that the edge e connects or joins the nodes u and v. Any pair of nodes which is connected by an edge in a graph is called adjacent to an edge.

1.5.3 Definition

In a graph $G = (E, V)$, an edge which is associated with an ordered pair of $V \times V$ is called a directed edge of G, while an edge which is associated with an unordered pair of nodes is called an undirected edge.

In the figure 1.5.1 we have edges e_1, e_2, and e_6 are directed. But edges e_3,e_4,e_5,e_7 and e_8 are undirected.

1.5.4 Definition

A graph in which every edge is directed is called a directed graph (a digraph), and if every edge is undirected then a graph is called an undirected graph. But if some edges are directed and some are undirected then a graph is called mixed.

1.5.5 Definition

An edge of a graph with identical ends is called a loop.
The direction of a loop is of no significance; hence it can be considered either a directed or an undirected edge.
For example e_3 in figure 1.5.1 is a loop.

1.5.6 Definition

A graph is simple if it has no loops and no two of its edges join the same pair of vertices.
So the graph in example (1.5.2) is not a simple graph. But the graph in the next figure is a simple (and directed) graph.

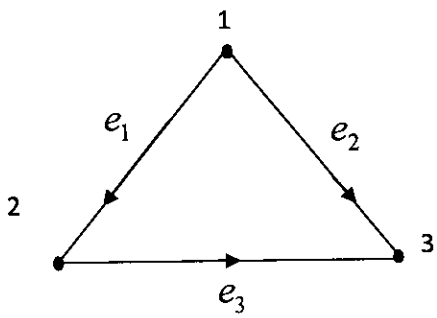


Figure 1.5.2 A diagram of the simple graph G.

1.5.7 Definition

A trivial graph is a graph which has just one vertex.

1.5.8 Definition

The graph with finite number of vertices as well as a finite number of edges is called a finite graph; otherwise, it is an infinite graph.

1.5.9 Definition

A vertex v_i and an edge e_j are said to be incident with each other, when v_i is an end vertex of e_j.

In figure 1.4.1, e_1, e_2 ,e_5 ,e_7 and e_8 are incident with the vertex v_2.

1.5.10 Definition

For a graph G, a walk is a finite alternating sequence of vertices and edges that begins and ends with a vertex and no edge appears more than once. The number of edges is called the length of the walk.

A vertex however, may appear more than once. Any edge that appears in a walk is incident to the preceding vertex and to the next vertex.

In figure 1.5.3, for example, $v_1 a v_2 b v_3 c v_3 d v_4 e v_2 f v_5$ is a walk.

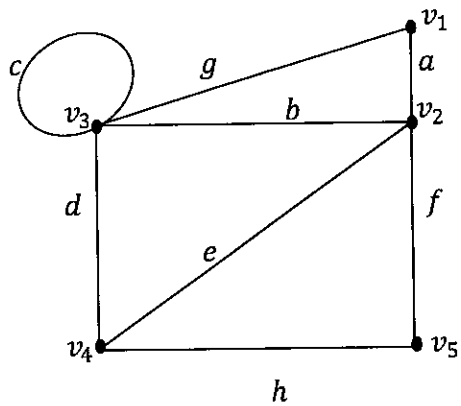


Figure 1.5.3

1.5.11 Definition

The net length of a walk is the difference between the number of forward edges and the number of backward edges, in the walk. Note that the net length may be negative.

1.5.12 Definition

A closed walk is a walk that begins and ends with the same vertex, and a walk that is not closed is called an open walk.

1.5.13 Definition

A path is an open walk in which no vertex appears more than once, and the length of a path is the number of edges in that path.

In figure 1.5.3, for example; $v_4 e v_2 f v_5$ is a path of length 2.

1.5.14 Definition

The distance between two vertices u and v in a graph G is the length of the shortest path joining them. It will be denoted by $d(u, v)$. If there is no path between u and v, then we say $d(u, v) = \infty$.

1.5.15 Definition

For a graph G, the diameter of G is denoted by $diam(G)$ and is defined by $diam(G) = sup\{d(u, v): u \neq v, and\, u, v \in G\}$.

1.5.16 Definition

A cycle is a closed walk such that no vertex (except the initial and the final vertex) appears more than once. A cycle is also called a circuit.

1.5.17 Definition

For a graph G, the girth of G is denoted by $gr(G)$ and is defined as the length of the shortest cycle in G. If there are no cycles in G, then we say $gr(G) = \infty$.

1.5.18 Definition

A graph G is called a connected graph if there is at least one path between any pair of vertices in G. Otherwise, G is called disconnected.

For instance, in figure 1.5.2, the graph is connected, while in figure 1.4.4, the graph is disconnected.

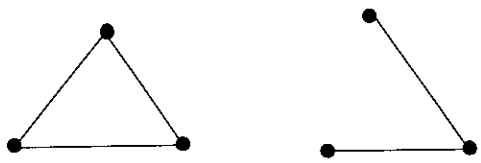


Figure 1.5.4 A diagram of A disconnected graph G

1.5.19 Definition

A graph G is called a complete graph if every pair of its vertices are adjacent.

A complete graph of n vertices is denoted by K_n, K_n has $\binom{n}{2}$ edges.

1.5.20 Example

The following is, K_4 complete graph

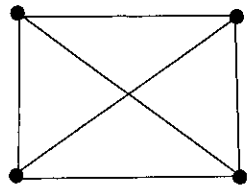


Figure 1.5.5 A diagram of the complete graph K_4

1.5.21 Definition

For a graph G, G is a bipartite graph if its vertex set V can be partitioned into two disjoint subsets V_1 and V_2 such that, every edge of G joins a vertex of V_1 with a vertex of V_2.

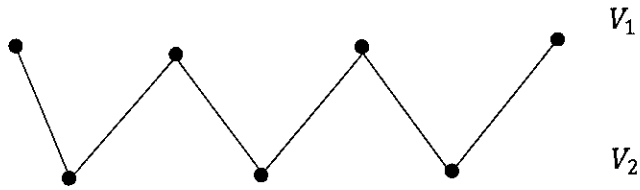


Figure 1.5.6 A diagram of a bipartite graph

If every vertex in V_1 is joined to every vertex in V_2 we obtain a complete bipartite graph. We write $K_{m,n}$ for the complete bipartite graph with $|V_1| = m$ and $|V_2| = n$. Here $|E| = mn$.

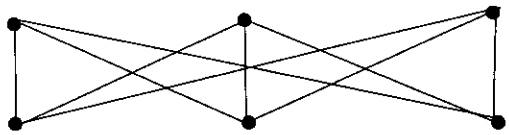


Figure 1.5.7 A diagram of the $K_{3,3}$ graph

1.5.22 Definition

A planar graph is one that can be drawn on a plane in such a way that there are no "edge crossings," i.e. edges intersect only at their common vertices.

1.5.23 Theorem (Kuratowski 1930)

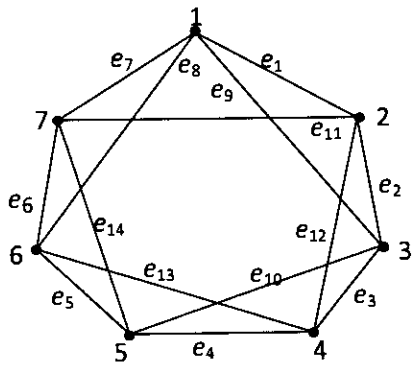
A finite graph G is planar if and only if it has no subgraph that is isomorphic to the complete graph in five vertices K_5 or the complete bipartite graph $K_{3,3}$.

1.5.24 Definition

Graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$ are isomorphic if there is a bijective function f from V_G to V_H such that for all vertices u and v in V_G , $(u, v) \in E_G$ if and only if $(f(u), f(v)) \in E_H$. And we write $G \cong H$.

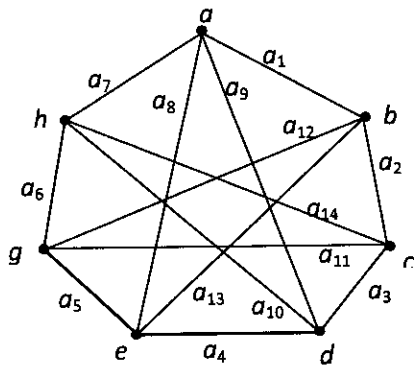
1.5.25 Example

Let G and H be the two graphs indicated in figures 1.5.8 and 1.5.9



G

Figure 1.5.8



H

Figure 1.5.9

Let $f: G \to H$ defined by:
$f(e_1) = a_9$, $f(e_2) = a_{10}$, $f(e_3) = a_{14}$, $f(e_4) = a_{11}$, $f(e_5) = a_{12}$, $f(e_6) = a_{13}$, $f(e_7) = a_8$, $f(e_8) = a_1$, $f(e_9) = a_7$, $f(e_{10}) = a_6$, $f(e_{11}) = a_4$, $f(e_{12}) = a_3$, $f(e_{13}) = a_2$, and $f(e_{14}) = a_5$.
Then f is the bijective function from V_G to V_H satisfy the following condition:
For all vertices u and v in V_G , $(u, v) \in E_G$ if and only if $(f(u), f(v)) \in E_H$.
And hence $G \cong H$.
Figure 1.5.10 gives another diagram of the graph G in the above example

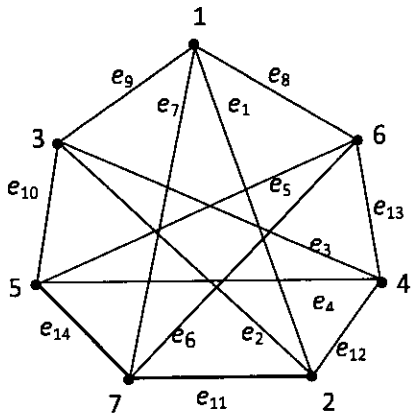


Figure 1.5.10

As a matter of fact all of our concentration will be on a homomorphism of graphs instead of isomorphism of graphs which will ignore the bijectivity, see definition 3.3.1 in the Chapter III.

1.5.26 Definition

A tree is a connected graph with no cycles. A spanning tree of a graph G is a subgraph of G which is a tree and includes all the nodes of G.

1.5.27 Example

In this example the tree has 6 vertices and $6 - 1 = 5$ edges. The unique simple path connecting the vertices 2 and 6 is 2456.

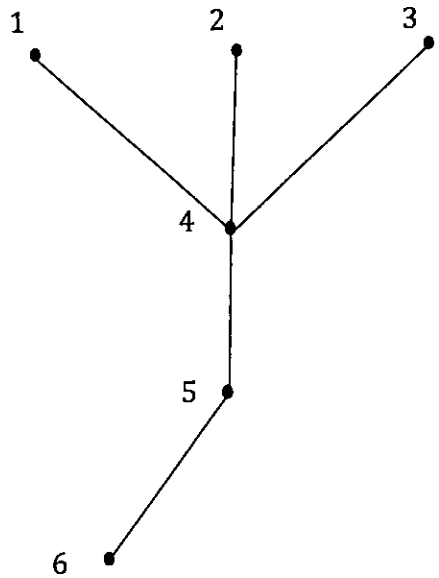


Figure 1.5.11 a diagram of tree

1.5.28 Definition

In an undirected tree, a leaf is a vertex of degree 1.

1.5.29 Theorem

Every tree has at least 2 leaves.

Proof

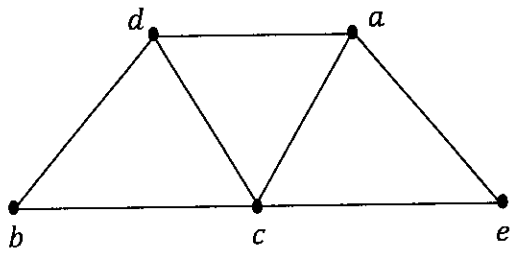
Let T be a tree and $P : u_1, u_2, \ldots, u_k$ a longest path in T. We know that P is not closed because T is a tree. We know that u_1 has degree 1 because if u_1 was adjacent to any vertex not on P, we would have a longer path and it can't be adjacent to any vertex on P other than u_2 or we would have a cycle. Similarly, u_2 must have degree 1.

1.5.30 Corollary

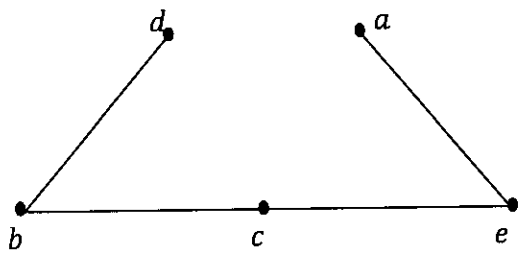
If the minimum degree of a graph is at least 2, then that graph must contain a cycle. ■

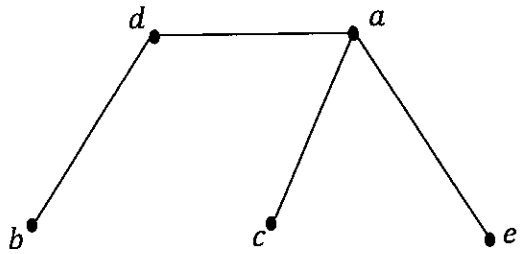
1.5.31 Example

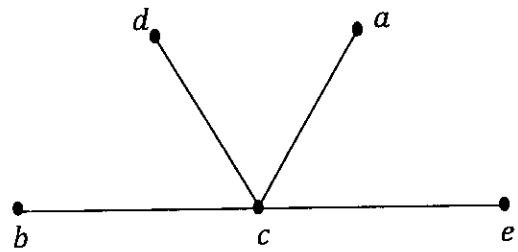
Consider the following graph G



The three spanning trees G are:







Chapter II

Graphs associated with rings

Introduction

In this chapter I will give some connections between commutative ring theory and graph theory which is very useful to understand a given algebraic structure R.

2.1 Zero-divisor graph

The idea of a zero-divisor graph of a commutative ring was introduced by I. Beck in [13] where he was mainly interested in coloring of commutative ring. This investigation of colorings of a commutative ring was then continued by D. F. Anderson and M. Naseer in [8].

2.1.1 Definition

An element x in a ring R is called a zero-divisor if there exist a non-zero element y in R such that $xy = 0$.

2.1.2 Definition (Anderson and Livingston graph $\Gamma(R)$)

Let R be a commutative ring with 1, and let $Z(R)$ be its set of zero-divisors. We associate a (simple) graph $\Gamma(R)$ to R with vertices $Z(R)^* = Z(R)\backslash\{0\}$, the set of non-zero zero-divisors of R, and for distinct $x, y \in Z(R)^*$, the vertices x and y are adjacent if $x\,y = 0$.

Thus $\Gamma(R)$ is the empty graph if and only if R is an integral domain.

2.1.3 Example

Below is the zero-divisor graph for $(\mathbb{Z}_6, +, \cdot)$ and $(\mathbb{Z}_8, +, \cdot)$.

Note that this example shows that nonisomorphic rings may have the same zero-divisor graph.

2.1.4 Theorem ([9], Theorem 2.2)

Let R be a commutative ring. Then $\Gamma(R)$ is finite if and only if either R is finite or an integral domain.

2.1.5 Theorem ([9], Theorem 2.3)

Let R be a commutative ring. Then $\Gamma(R)$ is connected and $Diam\,\Gamma(R) \leq 3$.

2.1.6 Theorem ([9], Theorem 2.4)

Let R be a commutative ring not necessarily with identity. If $\Gamma(R)$ contains a cycle, then $gr\Gamma(R) \leq 4$.

2.1.7 Theorem

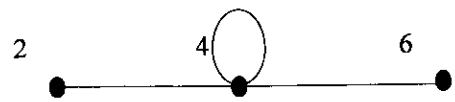
Let R be a commutative ring. Then $\Gamma(R)$ is complete if and only if either $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ or $xy = 0$ for all $x, y \in Z(R)$.

2.1.8 Definition

For any $x, y \in Z(R)$, define $x \sim y \;iff\; x\,y = 0 \;or\; x = y$. The relation $\sim$ is always reflexive and symmetric, but usually not transitive. The zero-divisor graph $\Gamma(R)$ measures this lack of transitivity in the sense that $\sim$ is transitive if and only if $\Gamma(R)$ is complete. (Not all graphs under this condition are simple).

2.1.9 Example

In [Example 2.1.3], the zero divisor graph for $(\mathbb{Z}_8, +, \cdot)$ will have a loop, because $4 \times 4 = 16 \equiv 0 \bmod 8$. The diagram will change as the following:



2.2 Comaximal graphs

2.2.1 Definition

A comaximal graph denoted by $\Omega(R)$ is the graph obtained by setting all the elements of R to be the vertices and defining distinct vertices x and y to be adjacent if and only if $Rx + Ry = R$.

In the following, $J(R)$ will be refries to the Jacobson radical of R, $U(R)$ is the group of units of R , $I(R)$ is the set of idempotents in R, and $Max(R)$ is the set of maximal ideals of R. And if we suppose that $\Omega_1(R) =< U(R) >$ and $\Omega_2(R) =< R \setminus U(R) >$ then we can give some properties of $\Omega(R)$ as in the following theorems:

2.2.2 Theorem ([15], Theorem 2.2)

Let R be a commutative ring. Then the following statements are equivalent:

(a) The graph $\Omega_2(R) \setminus J(R)$ is completely bipartite.

(b) $|Max(R)| = 2$.

2.2.3 Theorem ([15], Proposition 2.3)

Let R be a commutative ring and let $n > 1$. Then the following statements hold:

(a) If $|Max(R)| = n < \infty$, then the graph $\Omega_2(R) \setminus J(R)$ is n-partite.

(b) If $|Max(R)| \geq 2$ and the graph $\Omega_2(R) \setminus J(R)$ is n-partite, then $|Max(R)| \leq n$. In this case, if the graph $\Omega_2(R) \setminus J(R)$ is not $(n-1)$-partite, then $|Max(R)| = n$.

2.2.4 Theorem ([15], Proposition 2.4)

Let R be a commutative ring with $|Max(R)| \geq 2$. Then the following statements hold:

(a) If the graph $\Omega_2(R) \setminus J(R)$ is complete n-partite, then $n = 2$.

(b) If there exists a vertex of the graph $\Omega_2(R) \setminus J(R)$, which is adjacent to its every other vertex, then $R \cong \mathbb{Z}_2 \times \mathcal{F}$, where $\mathcal{F}$ is a field.

2.2.5 Theorem ([15], Theorem 3.1, Lemma 3.2, and Proposition 3.3)

Let R be a commutative ring. Then the graph $\Omega_2(R) \setminus J(R)$ is connected and we have $diam(\Omega_2(R) \setminus J(R)) \leq 3$. Moreover, $diam(\Omega_2(R) \setminus J(R)) = 1$ if and only if $R \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also if $|Max(R)| \geq 2$, then $diam(\Omega_2(R) \setminus J(R)) = 2$ if and only if one of the following statements hold:

(a) The Jacobson radical $J(R)$ is a prime ideal of R.

(b) $|Max(R)| = 2$ and $R \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2.3 Intersection ideal graphs

2.3.1 Definition

Let $F = \{S_i : i \in I\}$ be an arbitrary family of sets. The intersection graph $G(F)$ of F is the graph whose vertices are $S_i, i \in I$ and in which the vertices S_i and S_j $(i, j \in I)$ are adjacent if and only if $S_i \neq S_j$ and $S_i \cap S_j \neq \emptyset$.

We will denote to the intersection graph of ideals of R by $In(R)$. From the last definition it is clear that $In(R)$ is the undirected simple graph and its vertices are in a one-to-one correspondence with all nontrivial left ideals of R and two distinct vertices are joined by an edge if and only if the corresponding left ideals of R have a nontrivial (nonzero) intersection. Clearly the set of vertices is empty for left simple rings. In this case we refer $In(R)$ as the empty graph. Also for any ideal I in R we will give the same symbolize I to refer to the vertex in $In(R)$ which is corresponded to I.

The following is Lemma 2.1 in [16]

2.3.2 Lemma

If $\mathrm{In}(R)$ is planar, then any chain of ideals of R has length at most five.

2.3.3 Lemma ([16], Lemma 2.6)

If $In(R)$ is planar, then $|Max(R)| \leq 3$.

Chapter III

An interesting relationship between finite rings and graphs

Introduction

If we have a finite commutative ring R and $\emptyset: R^2 \to R^2$ is a mapping, where $\emptyset(a,b) = (a+b, ab)$ for all $a, b \in R$, then $\emptyset$ defines a finite directed graph $G = G(R)$, with vertices R^2 and edges defined by $\emptyset$. We will call it a ring graph, and under this connection we can connect some ring properties of R to graph properties of G. The basic of this work will be on rings $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, their graphs should reflect number-theoretic properties of integers.

3.1 Degrees and Vertices

In this work, we consider the degrees of vertices in $G(\mathbb{Z}_n)$. As usual, the outgoing (incoming) degree of a vertex (a,b) is the number of arrows going out (coming in) this vertex, since G is a function, so it is clear that the outgoing degree of each vertex is one. One might ask what the incoming degree of the vertex (a,b) is. The answer to this question was given in [5] as the following proposition.

3.1.1 Proposition

The incoming degree of the vertex $(a,b) \in G$ equals the number of distinct roots of the quadratic polynomial $X^2 - aX + b \in R[X]$.

If p is a prime, then the incoming degree of a vertex (a,b) in the graph G_p can be either 0 ($if\ X^2 - aX + b$ is irreducible, i.e., $0 \neq 4b - a^2 \in \mathbb{Z}_p$ is a quadratic non-residue modulo p), or 1 ($if\ 4b - a^2 = 0$), or 2 ($if\ 4b - a^2 \neq 0$ is a quadratic residue modulo p).

If n is a nonprime, then the incoming degree of a vertex (a,b) in the graph G_p can be greater than 2, which depends on the different factorizations of $X^2 - aX + b$. (As we will see in Figure 3.1 when $n = 6$, incoming degree is equal to 4).

3.1.2 Definition

The sequence:

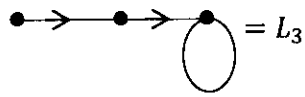
(3.1) $$(a_1, b_1) \to (a_2, b_2) \to \cdots \to (a_k, b_k)$$

of edges in G defines a cycle of length k (or a k-cycle) if $(a_k + b_k, a_k b_k) = (a_1, b_1)$ and $(a_i + b_i, a_i b_i) \neq (a_j, b_j)$ for all $j \leq i < k$. In addition, $\vec{C}_k$ will be referred to the directed cycle with vertices $0, 1, \ldots, k-1$.

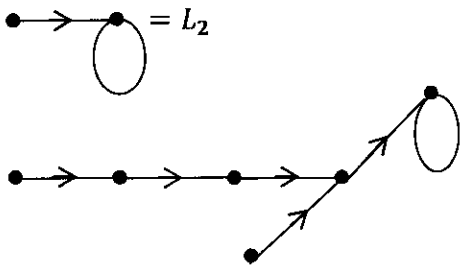
In the following diagram; $G_i = G(\mathbb{Z}_i)$ for $i = 1, 2, 3, 4, 5$, and 6. We notice that there are cycles of length one (loops) as well as longer cycles. Also, some graphs G_i do contain G_1 as a (weakly) connected component and some do not. The definition also implies that if $k > 1$, then every $b_i \neq 0$.

G_1:

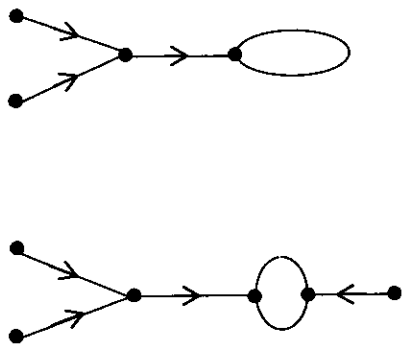
G_2:G_1 +



G_3:G_1 +



G_4:$3L_2$ +



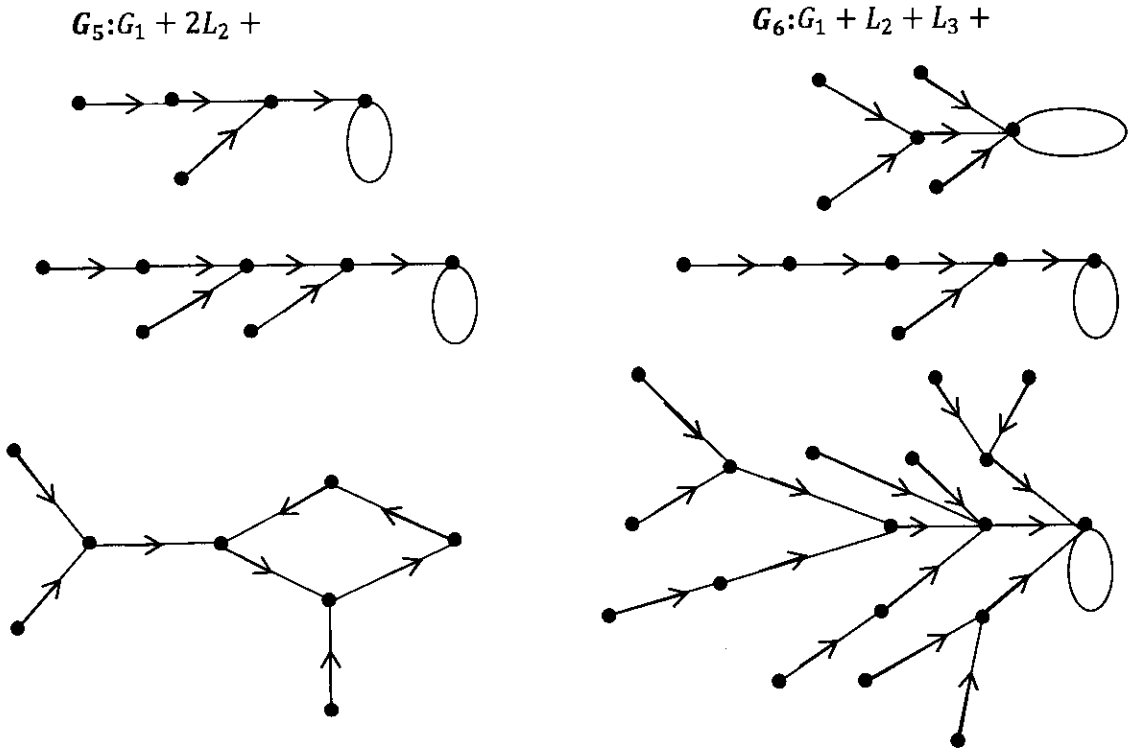


Figure 3.1

The following are propositions 3.1, 3.2 and 3.3 in [5].

3.1.3 Proposition

1) There are exactly $n = \#R$ cycles of length 1 (or loops) in G, and they correspond to the vertices $(a, 0)$.

2) Each connected component of G contains exactly one cycle, and the number of connected components is $n + \#\{cycles\ of\ length > 1\}$.

3) The graph G_1 is a (weakly) connected component of G if and only if R has no nontrivial nilpotent elements.

Actually the n components corresponding to loops are trees, with these loops as roots. Cycles of length greeter than 1 correspond to non-tree components, and the graph G is a union of these two paths: $G = T \cup N$. [T refers to tree and N refers to non-tree].

3.1.4 Proposition

If the sequence (3.1) is a k-cycle, then

$$\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0, \ \ (\sigma_k(a) - 1)\sigma_k(b) = 0$$

where $\sigma_m(X) = \sigma_m(X_1, \ldots, X_k) = \sigma_m^k$ are the usual elementary symmetric polynomials in k variables.

3.1.5 Proposition

For $k = 1$, the "sequence" (3.1) is a 1-cycle (or loop) $\Leftrightarrow \sigma_1(b) = 0$.
For $k = 2$, the sequence (3.1) is a 2- cycle $\Leftrightarrow \sigma_1(b) = \sigma_2(b) = 0$.
For $k = 3$, the sequence (3.1) is a 3- cycle $\Leftrightarrow \sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$.

3.1.6 Remarks

1) It is easy to see that there exists a 2- cycle $\Leftrightarrow$ the ring R has nontrivial nilpotent elements. For, since $(a_2, b_2) \neq (a_1, b_1)$, we have $b_1 \neq 0$, $b_1^2 = 0$ and this is a nilpotent in R. Conversely, if c is a nilpotent, $c^{k-1} \neq 0, c^k = 0$ for $k > 1$, take $b = c^{k-1}$. Then $b^2 = 0$ and there is a 2- cycle $(-1, b) \to (b - 1, -b) \to (-1, b)$. Therefore, the existence of nilpotents in R is visible in the graph G in two different, equivalent ways: the absence of a G_1-component and the presence of 2- cycle.

2) In the case $R = \mathbb{Z}_n$, this is equivalent to the condition that n is not square free, since $\mathbb{Z}_n$ has no nontrivial nilpotents if and only if n is square-free. This leads to an (inefficient) algorithm for deciding whether a given integer n is square-free: look for 2-cycle in the corresponding graph G_n.

3) The existence of a 3- cycle implies that the ring R has zero-divisors, since in such case $b_1 b_2 b_3 = 0$ and all $b_i \neq 0$.

4) Proposition 3.1.3 suggests a tempting conjecture: if the sequence (3.1) is a k-loop, then $\sigma_1(b) = \sigma_2(b) = \cdots = \sigma_k(b) = 0$. However, as the example $R = \mathbb{Z}_5$ shows (see Figure 3.1), it is already false for $k = 4$: there is a 4-cycle $(2, 2) \to (4, 4) \to (3, 1) \to (4, 3)$ such that $\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$ and $\sigma_4(b) \neq 0$. In this case, $\sigma_4(b) = 1$ in accordance with the proposition.

3.2 A Connection between a zero-divisor graph $\Gamma(R)$ and a ring graph $G(R)$

Let $\Gamma(R)$ be a zero-divisor graph defined as in [Definition 2.1.8]. Suppose that $a, b \in \Gamma(R)$ are adjacent vertices, which means that $ab = 0$. Now we have two cases:

(1): If $a \neq b$, then $ab = ba = 0 \Rightarrow \emptyset(a, b) = \emptyset(b, a) = (a + b, ab) = (a + b, 0)$, and

then $\emptyset(a+b,0) = (a+b,0)$ is a loop in the ring graph $G(R)$.

(2): If $a = b$, then a is an idempotent element in R and thus $a^2 = 0 \Rightarrow \emptyset(a,a) = (2a,0)$, and then $\emptyset(2a,0) = (2a,0)$ is also a loop in the ring graph $G(R)$.

These two cases can be explained as in the following diagram:

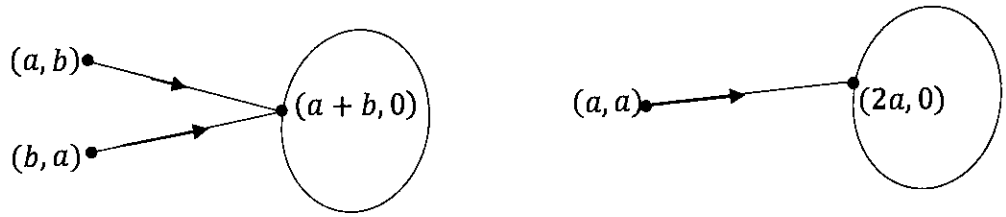


Figure 3.2

From figure 3.2 we can notice that an edge of a nonzero zero-divisor graph corresponds to a point in a tree component! [In a non-tree component there are no zero-divisors]. Moreover nonzero zero-divisors must be on level 2 in each tree component and level 1 consists of n points$(a,0)$, $a \in R$, so if we have a zero-divisor graph $\Gamma(R)$ then all vertices in both cases *(1)*, *(2)* must be on level 2 of the graph $G(R)$, also don't forget vertices of the form $(0,a)$, for all $a \in R$, $a \neq 0$. Because $\emptyset(0,a) = (a,0)$, and then $\emptyset(a,0) = (a,0)$ are loops in $G(R)$ for all $a \in R$ which are $(n-1)$ cases in a finite ring R with $|R| = n$. [i.e. vertices $(0,a), a \in R$ are also on level 2 in $G(R)$].

If we refer to the number of vertices of level 2 in $G(R)$ by μ, the number of edges in $\Gamma(R)$ by n_e, and the number of loops in $\Gamma(R)$ by n_l, then we can conclude the following proposition from the above argument.

3.2.1 Proposition

Let R be a finite ring with n elements, and suppose that $\Gamma(R)$, $G(R)$ are its nonzero zero-divisor graph and ring graph respectively. Then

$\mu = (n-1) + 2n_e + n_l$.

3.2.2 Example

Suppose that $R = (\mathbb{Z}_6, +, \cdot)$. Then by Example 2.1.3 we have $n_e = 2$ and $n_l = 0$, so $\mu = (6-1) + 2 \times 2 + 0 = 9$ which is the number of vertices of level 2 in $G(\mathbb{Z}_6) = G_6$. See (Figure 3.1) to check.

3.3 Homomorphism of graphs

3.3.1 Definition

A homomorphism of G to H, is a mapping $f: V(G) \to V(H)$ from G to H, such that it preserves edges, that is, if for any edge (u, v) of G,$(f(u), f(v))$ is an edge of H. We write simply $G \to H$.

If f is any homomorphism of G to H, then the digraph with vertices $f(v), v \in V(G)$, and edges $f(v)f(w)$, $vw \in E(G)$ is a homomorphic image of G. Note that $f(G)$ is a total subgraph of H, and that $f: G \to f(G)$ is a surjective homomorphism.

3.3.2 Proposition

Let G and H be digraphs, and $f: G \to H$ a homomorphism. If $v_0, v_1, \cdots, v_{k-1}$ is a walk in G, then $f(v_0), f(v_1), \cdots, f(v_{k-1})$ is a walk in H, of the same net length ([14]).

In particular, homomorphisms of G to H map paths in G to walks in H, and hence do not increase distances (the minimum length of the paths connecting two vertices). So we have the following fact.

3.3.3 Corollary

If $f: G \to H$ is a homomorphism, then $d(f(u), f(v)) \leq d(u, v)$, for any two vertices u, v of G.

Proof

If $u = v_0, v_1, \cdots, v_k = v$ is a path in G, then $f(u) = f(v_0), f(v_1), \cdots, f(v_k) = f(v)$ is a walk of the same length k in H. Since every walk from $f(u)$ to $f(v)$ contains a path from $f(u)$ to $f(v)$, we must have $d(f(u), f(v)) \leq k$. ■

3.3.4 Definition

The graph with vertices $v_0, v_1, \ldots, v_{k-1}$ and edges $v_i v_{i+1}$ for $i = 0, 1, \ldots, k-1$ (with addition mod k) is called the cycle $\vec{C}_k$. Note that $\vec{C}_k$ has k vertices and k edges.

3.3.5 Corollary

A mapping $f: V(\vec{C}_k) \to V(G)$ is a homomorphism of $\vec{C}_k$ to G if and only if $f(v_0)$, $f(v_1), \ldots, f(v_{k-1})$ is a closed walk in G.

Proof

Suppose that $\vec{C}_k$ is a cycle of distinct vertices $v_0, v_1, \ldots, v_{k-1}$. Then v_i and v_{i+1} are adjacent for all $i = 0, 1, \ldots, k-1$ (with addition mod k). By the Definition 3.2.1, $f: V(\vec{C}_k) \to V(G)$ is a homomorphism of $\vec{C}_k$ to G if and only if $f(a_i)$ and $f(a_{i+1})$ are adjacent for all $i = 0, 1, \ldots, k-1$ (including $f(v_{k-1})$ and $f(v_0)$), if and only if $f(v_0), f(v_1), \ldots, f(v_{k-1})$ is a closed walk in G. ■

3.3.6 Remark

In the case of $G = G(R)$ every closed walk is a cycle.

Proof: Obviously, since the out-degree is always 1. ■

Observe that a set of vertices is independent in G if it contains no pair of adjacent vertices. In terms of the associated partition, we have the following condition. A given digraph G satisfies $G \to \vec{C}_k$ if and only if the vertices of G can be partitioned into k independent sets $S_0, S_1, \ldots, S_{k-1}$ so that each edge of G goes from S_i to S_{i+1} for some $i = 0, 1, \ldots, k-1$ (with addition modulo k).

Recalling that a closed walk is a homomorphic image of a cycle, we can reformulate the last result as follows.

3.3.7 Corollary

A digraph G satisfies $G \to \vec{C}_k$ if and only if the net length of every closed walk in G is divisible by k. [See reference 14, page 6].

3.3.8 Corollary

$C_{2k+1} \to C_{2l+1}$ if and only if $l \leq k$.

Proof

An odd cycle has no closed odd walk shorter than its length, and has a closed walk of any odd length greater than or equal to its length. ■

Figure 3.3 illustrates a homomorphism $f: C_7 \to C_5$; the images $f(v), v \in V(C_7)$ are shown in C_5. (Hence we see the closed walk $f(0), f(1), \ldots, f(6), f(0)$ *in* C_5).

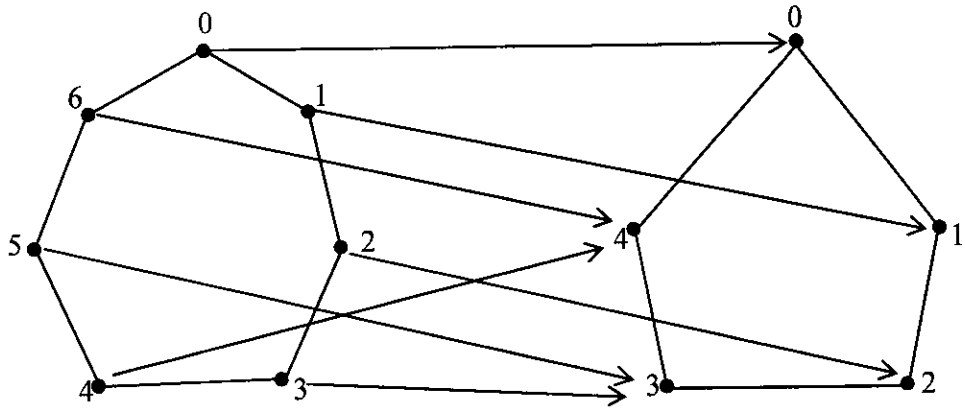


Figure 3.3

3.4 Related Properties

3.4.1 Theorem

$f = \{([a]_n, [a]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m | a \in \mathbb{Z}\}$ is a function $f: \mathbb{Z}_n \to \mathbb{Z}_m$ if and only if $m \mid n$.

Proof. See in [7, p. 89]. ■

Let m and k be relatively prime numbers, such that $n = m.k, m < k$. Define a map

$$h_1: \mathbb{Z}_n \to \mathbb{Z}_m$$

that maps representative $0 \leq a < n$ in $\mathbb{Z}_n$ to $(a \bmod m)$ in $\mathbb{Z}_m$. Since m divides n, then h_1 is a homomorphism. Moreover, $ker h_1 = m\mathbb{Z}_n < \mathbb{Z}_n$, and $|ker h_1| = k$.

Similarly, the same holds for $h_2: \mathbb{Z}_n \to \mathbb{Z}_k$.

. Observe that mappings h_1 and h_2 induce mappings of corresponding graphs, which will be denoted again by h_1 and h_2, $h_1: G(\mathbb{Z}_n) \to G(\mathbb{Z}_m)$, $h_2: G(\mathbb{Z}_n) \to G(\mathbb{Z}_k)$.

We will denote the longest cycle in the digraph $G(\mathbb{Z}_n)$ by $\vec{C}_{l_n}$ for short (We should notice that G may have more than one cycle of the same longest length l_n), and all our discussion later will be based on the construction of h_1 and h_2.

3.4.2 Proposition

Let $\vec{C}_{l_n}$ and $\vec{C}_{l_m}$ be two directed cycles in $G(\mathbb{Z}_n)$ and $G(\mathbb{Z}_m)$ respectively. If $\vec{C}_{l_n} \to \vec{C}_{l_m}$, then l_m divides l_n.

Proof

Suppose that $\vec{C}_{l_n}$ is a s-cycle (where $s = l_n$); that is,

$(a_1, b_1) \to (a_2, b_2) \to \cdots \to (a_s, b_s)$.

Since h_1 is a homomorphism, then

$$(h_1(a_1), h_1(b_1)) \to (h_1(a_2), h_1(b_2)) \to \cdots \to (h_1(a_s), h_1(b_s))$$

is a cycle in $G(\mathbb{Z}_m)$, and

$$(h_1(a_1), h_1(b_1)) = (h_1(a_s + b_s), h_1(a_s \cdot b_s))$$

$$= (h_1(a_s) + h_1(b_s), h_1(a_s) \cdot h_1(b_s)) \quad (1)$$

Since h_1 connects k elements in $\mathbb{Z}_n$ into every element $a \in \mathbb{Z}_m$, that means $(h_1(a_1), h_1(b_1)) = (h_1(a_j), h_1(b_j))$, for some $2 \le j \le s$. Then $(h_1(a_i), h_1(b_i)), i < j$ are all different. So according to (1) $l_n = t.l_m$, for $1 \le t \le s$. Hence l_n is divisible by l_m. ■

In the following we will use the so-called *Chinese Reminder Theorem*:

3.4.3 Theorem (Chinese Reminder Theorem)

Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ be pairwise relatively prime numbers, i.e., $gcd(n_i, n_j) = 1$ for $i \neq j$. Let $n = n_1 n_2 \ldots n_r$. Then the map

$$\psi: \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}, [x] \to ([x \bmod n_1], \ldots, [x \bmod n_r])$$

is an isomorphism of rings.

Proof. (e.g [12]) ■

3.4.4 Proposition

If $n = m.k$, m and k are relatively prime numbers, then $G_n = G_m \times G_k$.

Proof

By Theorem 3.4.3, $\mathbb{Z}_n = \mathbb{Z}_m \times \mathbb{Z}_k$ and since $h_1: \mathbb{Z}_n \to \mathbb{Z}_m$, $h_2: \mathbb{Z}_n \to \mathbb{Z}_k$ define ring homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ and $\mathbb{Z}_k$ respectively, then $h_1: G(\mathbb{Z}_n) \to G(\mathbb{Z}_m)$, $h_2: G(\mathbb{Z}_n) \to G(\mathbb{Z}_k)$ also define graph homomorphisms. Hence $G_n = G_m \times G_k$.

3.4.5 Corollary

There is a bijection between cycles $\vec{C}_r$ in G_n and pairs of cycles $(\vec{C}_s, \vec{C}_t)$ in $G_m \times G_k$, where $r = LCM(s,t)$.

In the following proposition, if we suppose that $l_m | l_k, l_m \neq 1$ (so l_m might be equal to l_k) then there is no proof that maps h_1 and h_2 will send the longest cycle $\vec{C}_{l_n}$ in $G(\mathbb{Z}_n)$ to longest cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ in $G(\mathbb{Z}_m)$ and $G(\mathbb{Z}_k)$ respectively. Because the cycles in $G(\mathbb{Z}_m)$ and $G(\mathbb{Z}_k)$ which are smaller than $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ might have a pre-image which is a cycle with length longer than the pre-image of $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ themselves. As an example, suppose that $n = 17 \times 25 = 425$ so $m = 17$ and $k = 25$ then $\vec{C}_{l_m} = \vec{C}_{10}$, $\vec{C}_{l_k} = \vec{C}_5$ and the pre-image for both of them is $\vec{C}_{10}$ while the pre-image of cycles $\vec{C}_4 \in G(\mathbb{Z}_m)$ and $\vec{C}_5 \in G(\mathbb{Z}_k)$ is a cycle $\vec{C}_{20}$ which is longer than $\vec{C}_{10}$. So we will take in our consideration that if $l_m | l_k$, then l_m must be equal to 1.

3.4.6 Proposition

The maps h_1 and h_2 send the longest directed cycle $\vec{C}_{l_n}$ to the longest directed cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$, respectively.

Proof

Suppose that $\vec{C}_{l_m}, \vec{C}_{l_k}$ are longest cycles in $G(\mathbb{Z}_m)$ and $G(\mathbb{Z}_k)$ respectivaly. Then l_m, l_n will have only two possible cases:

Case (1) If $l_m = 1$, then $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ have the same pre-image. Let us call it $\vec{C}_r$, so $l_m | r, l_k | r$ (see proposition 3.4.2), and by Chinese Reminder Theorem $r = l_k$. Our goal now is to prove that $\vec{C}_r$ is the longest cycle in $G(\mathbb{Z}_n)$. Assume that there is an another cycle $\vec{C}_d \neq \vec{C}_r$ such that $d > r$, then the length of $h_1(\vec{C}_d)$ divides the length of $\vec{C}_d$, also the length of $h_2(\vec{C}_d)$ divides the length of $\vec{C}_d$. Then again by using Chinese Reminder Theorem we get $h_1(\vec{C}_d) > \vec{C}_{l_m}$ or $h_2(\vec{C}_d) > \vec{C}_{l_k}$ (This inequality holds if $h_1(\vec{C}_d)$ and $h_2(\vec{C}_d)$) are relatively primes or even if they are not relatively primes);
This contradicts our assumption, that $\vec{C}_{l_m}, \vec{C}_{l_k}$ are longest cycles.
Case (2) If $(l_m, l_k) = 1$. As we have done in the *case (1)*, the cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ will have the same pre-image $\vec{C}_r$ where $l_m | r$, and $l_k | r$. Suppose that there is an another cycle

$\vec{C}_q$ such that $q > r$, then the length of $h_1(\vec{C}_q)$ divides the length of $\vec{C}_q$ and the length of $h_2(\vec{C}_q)$ divides the length of $\vec{C}_q$ (see proposition 3.4.2).

- If the length of $h_1(\vec{C}_q) = l_m$, then the length of $h_2(\vec{C}_q) > l_k$. Similarly if $h_2(\vec{C}_q) = l_k$, then
  the length of $h_1(\vec{C}_q) > l_m$. Both cases contradict with our assumption.
- If the length of $h_1(\vec{C}_q) = 1$, in this case the length of $\vec{C}_q$ equals the length of $h_2(\vec{C}_q)$, which means $h_2(\vec{C}_q) > l_k$. This is a contradiction.
- If the length of $h_1(\vec{C}_q) < l_m$ and is not 1. Then $h_2(\vec{C}_q) > l_k$ because $\vec{C}_q > \vec{C}_r$. Where lengths of the last cycles is the product of $h_1(\vec{C}_q)$, $h_2(\vec{C}_q)$ and $\vec{C}_{l_m}, \vec{C}_{l_k}$ respectively. This case indicates a contradiction. Hence $\vec{C}_r$ is the longest cycle in $G(\mathbb{Z}_n)$.

So in both cases we have proved that $\vec{C}_r = \vec{C}_{l_n}$ which completes the prove ■

3.4.7 Corollary

All directed cycles $\vec{C}_p$, for all primes p are incomparable. i.e., $\vec{C}_p \to \vec{C}_q$ if and only if $p = q$.

3.4.8 Theorem

Let $m, k \in \mathbb{N}$ be relatively prime numbers, i.e., $gcd(m, k) = 1$. Let $n = mk$. Then, the length of the longest cycle $\vec{C}_{l_n}$ is the least common multiple of l_m and l_k, where l_m and l_k are the lengths of the longest cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ respectively.

Proof

We will use the theorem 3.4.1, and the argument below it. Consider that $\vec{C}_{l_n}$ is a s-cycle (where $s = l_n$), that is

$(a_1, b_1) \to (a_2, b_2) \to \cdots \to (a_s, b_s)$.

Then, $h_1(\vec{C}_{l_n})$ is a cycle in $G(\mathbb{Z}_m)$. Similarly, $h_2(\vec{C}_{l_n})$ is a cycle in $G(\mathbb{Z}_k)$. So according to propositions 3.4.2 and 3.4.6, we have the following cases:

(1) If $(a_1, b_1) \in \mathbb{Z}_m \times \mathbb{Z}_m \subset G(\mathbb{Z}_n)$. Then, both h_1 and h_2 send (a_1, b_1) to the same vertex, so that the cycle $\vec{C}_{l_n}$ must terminate at the first multiple of l_m and l_k, because (a_1, b_1) is a unique original vertex of $(h_1(a_1), h_1(b_1))$ and $(h_2(a_1), h_2(b_1))$.

(2) If $(a_1, b_1) \notin \mathbb{Z}_m \times \mathbb{Z}_m$. Then, the map h_1 sends the element t in $\mathbb{Z}_n$ to element (t mod m) in $\mathbb{Z}_m$. Similarly, the map h_2 sends the element t in $\mathbb{Z}_n$ to element (t mod k) in $\mathbb{Z}_k$. Since m and k are two different modules, by Chinese Remainder Theorem, two

different vertices $(h_1(a_1), h_1(b_1))$ and $(h_2(a_1), h_2(b_1))$ uniquely determine the original vertex (a_1, b_1). Thus the length of $\vec{C}_{l_n}$ terminates exactly at the first multiple of the lengths of $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$. Hence the proof follows. ■

3.4.9 Theorem

Let $p_1, p_2, \ldots, p_r \in \mathbb{N}$ be pairwise relatively prime numbers, i.e., $gcd(p_i, p_j) = 1$ for $i \neq j$. Let $n = p_1 \ldots p_r$. Then the longest cycle $\vec{C}_{l_n}$ in $G(\mathbb{Z}_n)$ has a length $l_n = LCM(l_{p_1}, l_{p_2}, \ldots, l_{p_r})$, where $l_{p_1}, l_{p_2}, \ldots, l_{p_r}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p_1}),, G(\mathbb{Z}_{p_2}),, \ldots, G(\mathbb{Z}_{p_r})$, respectively.

Proof

The proof follows directly from theorem 3.4.8 and Chinese Remainder Theorem, by mathematical induction on r. ■

3.4.10 Proposition

The length of the longest cycle $\vec{C}_{l_{p^m}}$ can be p^{m-1} or $\alpha \cdot r$ for some $\alpha > 1$, where r is the length of the cycle $\vec{C}_{l_{p^m}}$.

Proof

Let p be a prime number, and $m > 1$ be any integer. The function $h: \mathbb{Z}_{p^m} \to \mathbb{Z}_p$ which is defined by $h(a) = a \bmod p$ is a homomorphism, and $kerh = p\mathbb{Z}_{p^m} < \mathbb{Z}_{p^m}$, where $|kerh| = p^{m-1}$.

Suppose that

$$(a_1, b_1) \to (a_2, b_2) \to \cdots \to (a_s, b_s)$$

is the longest cycle $\vec{C}_{l_{p^m}}$ (where $l_{p^m} = s$) in $G(\mathbb{Z}_{p^m})$. Therefore, if $b_1 \in kerh$, then $h(\vec{C}_{l_{p^m}})$ will be $(a, 0)$, $a = h(a_1) \in \mathbb{Z}_p$. It follows that, $l_{p^m} \leq p^{m-1}$ (because p^{m-1} is the number of elements in $\mathbb{Z}_{p^m}$, which are congruent to a mod p), where l_{p^m} is the length of the cycle $\vec{C}_{l_{p^m}}$. To prove $l_{p^m} = p^{m-1}$ we will prove it for $m = 2$ and the complement comes by using the mathematical induction on m.

Let $m = 2 \Rightarrow s = l_{p^m} = l_{p^2}$, suppose that $b_1 = tp, 1 \leq t < p$ that means

(*) $(a_1, b_1) = (a_1, tp) \to (a_1 + tp, a_1 tp) \to \big(a_1 + tp + a_1 tp, (a_1 + tp)(a_1 tp)\big) \to$
$\cdots \to (a_1 + (1 + a_1 + a_1^2 + a_1^3 + \cdots + a_1^{p-2})tp, a_1^{p-1} tp)$

Since

$1 + a_1 + a_1^2 + a_1^3 + \cdots + a_1^{p-2} = \frac{a_1^{p-1}-1}{a_1-1}$,

then

$(a_1 + (1 + a_1 + a_1^2 + a_1^3 + \cdots + a_1^{p-2})tp, a_1^{p-1} tp) = (a_1 + \frac{a_1^{p-1}-1}{a_1-1} tp, a_1^{p-1} tp)$,

by (Theorem 1.4.2) we get,

$\left(a_1 + \frac{a_1^{p-1}-1}{a_1-1} tp, a_1^{p-1} tp\right) = (a_1, tp)$, and by the substitution in (*) we get:

$(a_1, b_1) \to (a_1 + tp, a_1 tp) \to \big(a_1 + tp + a_1 tp, (a_1 + tp)(a_1 tp)\big) \to \cdots \to (a_1, b_1)$

Hence $l_{p^m} = p^{2-1} = p$.

If $b_1 \notin kerh$, then a_1 won't be in $kerh$ neither. Assume that $h\left(\vec{C}_{l_{p^m}}\right) = \vec{C}_r$ that means $1 < r \leq l_p$. According to theorem 3.4.8, we observe that r divides l_{p^m}. Hence $l_{p^m} = \alpha\, r$ for some $\alpha > 1$. ■

Note that, at the moment there is no way to determine the value of α in the second case. For instance, when $n = 5$, 5-cycle is the longest cycle in $G(\mathbb{Z}_{25})$. At the same time, 4-cycle is the longest cycle in $G(\mathbb{Z}_5)$ [so it is case 1]. When $n = 11$, 30-cycle is the longest cycle in $G(\mathbb{Z}_{121})$. At the same time, 6-cycle is the longest cycle in $G(\mathbb{Z}_{11})$ [so it is case 2].

Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ be the decomposition of n into different primes. Then, according to theorem 3.4.3, $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_r}}$.

3.4.11 Theorem

Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ be the decomposition of n into primes, such that $p_i \neq p_j$ for $i \neq j$, Then, the longest cycle $\vec{C}_n$ of $G(\mathbb{Z}_n)$. Has length $l_n = LCM(l_{p_1^{n_1}}, l_{p_2^{n_2}}, \ldots l_{p_r^{n_r}})$, where $l_{p_1^{n_1}}, l_{p_2^{n_2}}, \ldots, l_{p_r^{n_r}}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p^{n_1}}), G(\mathbb{Z}_{p^{n_2}}), \ldots, G(\mathbb{Z}_{p^{n_r}})$ respectively.

Proof

The proof comes by using Chinese Remainder Theorem, the preceding argument, and Theorem 3.4.9. ■

Conclusions

The aim of this thesis is to find some an interesting relations between finite commutative rings with unity and there digraphs. The strategy was to define a digraph $G(\mathbb{Z}_n)$ on the finite ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ as follows:

Define a mapping $\varphi: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \times \mathbb{Z}_n$ by $\varphi(a,b) = (a+b, ab)$. Likely, this mapping reflects the structure of $\mathbb{Z}_n$. Since $\mathbb{Z}_n$ is finite, so one can interpret φ as finite digraph $G = G(\mathbb{Z}_n)$ with vertices $\mathbb{Z}_n \times \mathbb{Z}_n$ and arrows defined by φ. If n is not prime, then $\mathbb{Z}_n$ has zero-divisors and $\mathbb{Z}_n[X]$ is not a unique factorization ring (if $ab = 0$, $a \neq 0$, $b \neq 0$, then $(X-a)(X-b) = X[X-(a+b)]$ are two distinct, nonassociated factorization of $X^2 - (a+b)X$. If $n = p$ is prime, then $\mathbb{Z}_n$ nevertheless could have zero-divisors. From the above we see that either n is a prime, $\mathbb{Z}_n$ is a field and $\mathbb{Z}_n[X]$ is a UFD, or n is not prime, $\mathbb{Z}_n$ has zero-divisors and $\mathbb{Z}_n[X]$ does not have the UF property. Let m and k be relatively prime numbers, such that $n = mk$, $m < k$. Define two maps

$$h_1: \mathbb{Z}_n \to \mathbb{Z}_m,$$

$$h_2: \mathbb{Z}_n \to \mathbb{Z}_k.$$

This two maps representatives $0 \leq a < n$ in $\mathbb{Z}_n$to $(a \bmod m)$ in $\mathbb{Z}_m$ and $(a \bmod k)$ in $\mathbb{Z}_k$ respectively.

Observe that mappings h_1 and h_2 induce mappings of corresponding graphs, which will be denoted again by h_1 and h_1. Define the directed cycle $\vec{C}_k = 012 \ldots k-1$ in $G(\mathbb{Z}_n)$, likewise $\vec{C}_{l_n}$ will refer to the longest cycle in $G(\mathbb{Z}_n)$. By using a homomorphism graphs and Chinese Reminder Theorem, I will prove some properties like;

1) Let $\vec{C}_{l_n}$ and $\vec{C}_{l_m}$ be two directed cycles in $G(\mathbb{Z}_n)$ and $G(\mathbb{Z}_m)$ respectively. If $\vec{C}_{l_n} \to \vec{C}_m$, then we have l_m divides l_n.
2) If $n = m.k$, m and k are relatively prime numbers, then $G_n = G_m \times G_k$.
3) The maps h_1 and h_2 send the longest directed cycle $\vec{C}_{l_n}$ to the longest directed cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ respectively.
4) Let $m, k \in \mathbb{N}$ be relatively prime numbers, i.e., $gcd(m,k) = 1$. Let $n = mk$. Then, the length of the longest cycle $\vec{C}_{l_n}$ is the least common multiple of l_m and l_k, where l_m and l_k are the lengths of the longest cycles $\vec{C}_{l_m}$ and $\vec{C}_{l_k}$ respectively.

5) The length of the longest cycle $\vec{C}_{l_{p^m}}$ can be p^{m-1} or $\alpha \cdot r$ for some $\alpha > 1$, where r is the length of the cycle $\vec{C}_{l_{p^m}}$.

6) Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$ be the decomposition of n into primes, such that $p_i \neq p_j$ for $i \neq j$, Then, the longest cycle $\vec{C}_{l_n}$ of $G(\mathbb{Z}_n)$. has a length $l_n = LCM(l_{p_1^{n_1}}, l_{p_2^{n_2}}, \dots, l_{p_r^{n_r}})$, where $l_{p_1^{n_1}}, l_{p_2^{n_2}}, \dots, l_{p_r^{n_r}}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p^{n_1}}), G(\mathbb{Z}_{p^{n_2}}), \dots, G(\mathbb{Z}_{p^{n_r}})$ respectively.

References

[1] A.A. Mehrvarz and Samei, On Commutative Gelfand Rings, Sci. I. Iran, Vol. 10 No.3Summer 1999.

[2] A. Guillory, Realizing Zero-Divisor Graphs, SMILE (2011).

[3] A. J. Berrick and M. E. Keating, An Introduction to Rings and Modules, The Press Sundicate of the University of Cambridge (2000).

[4] Alberta, General Topology, Addison-Wesley Publishing Company, Inc. (1968).

[5] A. Lipkovski, Digraphs associated with rings and some integer functions, Publishings De L'Institut Mathematique, Nouvelle série, tome 92(106) (2012), 35–41.

[6] A. Lipkovski, O. Shafah, H. Daoub, Vychislenie grafov konechnyh kolec. Vrnjacka Banja Serbia-Budva Montenegro, August 27-September 5, 2011.

[7] C. Lansky, Concepts in abstract algebra, Thomson Brooks/Cole, USA, 2005.

[8] D. Anderson and M. Naseer, Beck's coloring of a commutative ring, Journal of algebra 159, 500-514 (1993).

[9] David F. Anderson and Philip S. Livingston, The Zero-Divisor Graph of a Commutative Ring, Journal of Algebra 217, 434-447 (1998).

[10] G. De Marco, A. Orsatti, Commutative rings in which every prime ideal is contained in a unique maximal ideal, Proc. Amer. Math. Soc 30 (1971) 459–466

[11] Hans Delfs and Helmut Knebl, Introduction to cryptography, Springer-Verlag Berlin Heidelberg 2007.

[12] H. Delfs, H. Knebl, Introduction to Cryptography, Principles and Applications. Second Edition, Springer-Verlag, Berlin Heidelberg, (2007).

[13] I. Beck, Coloring of commutative rings, J. Algebra 116 (1988) 208–226.

[14] J. Ball, D. Welsh, Graphs and Homomorphisms, Oxford University Press, New York, 2004.

[15] Maimani, H.R. Salimi, M. Sattari, A. Yassemi, Comaximal graph of commutative rings. J. Algebra 319(4), 1801–1808 (2008).

[16] Sayyed Heidar Jafari and Nader Jafari Rad, Planarity of intersection graphs of idea ls of rings, International electronic journal of algebra. Volume 8 (2010) 161-166.

[17] S.B. Mulay, Cycles and symmetries of zero-divisors, Comm. Algebra 30 (7) (2002) 3533–3558.

[18] S. B. Mulay, Rings having zero-divisor graphs of small diameter or large girth,Bull. Austral. Math. Soc. Vol. 72 (2005) [481-490].

[19] S. Shah, R. Sharma, and A. Shankar, Algebra I, Dorling Kindersley (India) Pvt. Ltd (2012).

[20] S. Silvestrov, Prim and maximal ideals, Spring term (2011).

[21] V. K. Bhat and Ravi Raina, A Note on zero divisor graph over rings, Int. J. Contemp. Math. Sci., Vol. 2, (2007), No. 14, 667-671.

Прилог 1.

Изјава о ауторству

Потписани-а Osama AB. M. Shafah

број уписа 2017/2008

Изјављујем

да је докторска дисертација под насловом

"Lipchitz space and quasiconformal mappings"

- **резултат сопственог истраживачког рада,**
- **да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,**
- **да су резултати коректно иаведени и**
- **да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.**

Потпис докторанда

У Београду, _____

_____

Прилог 2.

Изјава о истоветности штампане и електроиске верзије докторског рада

Име и презиме аутора : Osama AB. M. Shafah

Број индекса: _____

наслов рада : "An Interesting relationship between finite rings and graphs"

Ментор : Full Prof. dr Aleksandar Lipkovski

Потписани/ а Osama Abdel salam Mohamed Al Shafah

Изјавији да је штампана верзије мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијње академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду , _____

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

“Lipchitz space and quasiconformal mappings”

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, _____

_____

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo - nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo - nekomercijalno - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo - nekomercijalno - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju I javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.