Derivations on Semirings

Dissertation submitted to

Mahatma Gandhi University

in partial fulfillment of the requirements

for the award of the degree of

Master of Science in Mathematics

by

Nimna V J

Reg. No: 210011014844

under the supervision and guidance of

Prof.Aleena

Department of Mathematics

Bharata Mata College,Thrikkakkara, Kerala, India.

2021-2023

DECLARATION

I, Nimna V J, hereby declare that this dissertation entitled "DERIVATIONS ON SEMIRINGS" is an authentic record of the original work done by me under the guidance of Prof. Aleena, Assistant Professor, Department of Mathematics, Bharata Mata College, Thrikkakkara. I also declare, that this dissertation has not been submitted by me fully or partially for the awards of any degree, diploma, title or recognition earlier.

NIMNA V J

M.Sc. Mathematics

Bharata Mata College

Thrikkakkara

CERTIFICATE

Certified that this dissertation, **"DERIVATIONS ON SEMIRINGS"** is the bonafide work of **NIMNA V J** who carried out the project under my supervision.

Prof. Aleena

Assistant Professor

Submitted for the project viva-voice examination held on ....

INTERNAL EXAMINER	**EXTERNAL EXAMINER**
______________________	______________________

ACKNOWLEDGEMENT

I would like to take this opportunity to thank one and all who provided valuable advice and assistance, without which this project would not have been successful especially our beloved HOD Dr.Lakshmi M C and all other teachers in our department.

NIMNA V J

Contents

Introduction

A key component of mathematical sciences is widely regarded as abstract algebra. It deals with the investigation of algebraic entities such groups, rings, vector spaces, and algebras. With two binary operations that enjoy various features, the "semiring" algebraic structure is the most generalised. It is frequently regarded as a fundamental structure in abstract algebra, which defines the boundaries of the surrounding mathematical universe. Dedekind, Macaulay, and Krull began some of the implicit work in the creation of the semiring theory, but it was Vandiver who first proposed the idea of semirings openly. Since that time, numerous scholars have investigated various aspects of semirings and demonstrated that they have useful applications in the fields of theoretical computer science and mathematical sciences. Early in the 1950s, extensive research into the algebraic theory of semirings began, which sped up the development of the theory and its applications. In the areas of practical mathematics such as the theories of automata, formal languages, optimisation, and graph theory, a semiring naturally develops. The idea that a universal algebra with two associative binary operations, addition (often represented by +) and multiplication (typically denoted by . or by concatenation), where one of them distributes over the other, is called a semiring was first put forth by Vandiver in 1934. The necessity of neutral elements is relaxed by this definition. Semiring is a structure that doesn't require a 0 or 1 to exist, according to certain authors. As a result, the comparison between **group** and **semigroup** and **ring** and **semiring** works more effectively. These authors frequently use the term "rig" to refer to the idea here. The original joke here was that rigs are just rings without the negative elements. In a similar way, "rng" can also refer to a ring devoid of a multiplicative identity. As long as the concept of the derivative has existed, there have been fundamental and significant relationships between the operations of differentiation and addition and multiplication of functions. The study of algebraic structures with a finite number of derivations—linear functions that adhere to the Leibniz product rule—is the subject of differential algebra. Old and important in the integration of analysis, algebraic geometry, and algebra is The idea of the ring with derivation (i.e. with differentiation) plays an important role in algebra, algebraic geometry and integration of analysis. Although it was started years ago, the subject of ring derivations didn't really catch on until Posner published two extremely eye-catching findings on derivations in prime rings in 1957. Additionally, the concept of derivation has been generalised in a number of ways, including Jordan derivation, generalised Jordan derivation, etc. It was discovered in the 1940s that the Picard-Vessiot theory of ordinary linear differential equations can be applied to the Galois theory of algebraic equations. The classic texts on differential algebra were written by Ritt in 1950 and Kolchin in 1973. Numerous studies on derivations in rings, Lie rings, skew polynomial rings, and other structures have been conducted over the past few decades. An attempt has been made to provide insight into the theory and applications of semirings in this work.

The first chapter introduces the reader with a collection of notations and ideas in the form of definitions which can be used as ready reference for easy understanding of the subsequent topics. Starting from the idea of groups we finally reach the idea of semirings which we need throughout this paper.The second chapter gives a brief idea about derivations on rings and semirings and some lemmas relating to it. The third chapter gives the link between semiring theory and graph theory. Through this chapter we get an algorithm to find minimum path in a network. The last chapter helps us to relate the homomorphisms and derivations on semirings.

Chapter 1

SEMIRINGS

1.1 Groups

1.1. ***GROUP***[2] *$(G,*)$ is referred to as a* ***group*** *if G is a non-empty set and "$*$" is the binary operation defined on G such that the following laws or axioms are true.*

*(1)**closure law***

if for all $x, y \in G$, $x * y \in G$

*(2)**Associative law***

if $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$

*(3)**Identity element***

if there is an element $e \in G$ such that $x * e = e * x = x$ for all $x \in G$; where e is the identity element

*(4)**Inverse law***

if for each $x \in G$, there exists an element $y \in G$ such that $x * y = y * x = e$, where $y = x^-1$ is the inverse element of x

Example 1.1. *The algebraic structure started by natural numbers under the addition operation is denoted by the symbol $(\mathbb{N},+)$. However, because it does not adhere to the inverse law, $(\mathbb{N},+)$ is not a group. For instance, the inverse element of $3 \in \mathbb{N}$, given -3 in $\mathbb{N}$ with regard to $+$, does not exist.*

1.2. *ABELIAN GROUP* *If (G,$*$) has a binary operation that fulfils the commutative law, i.e., $a * b = b * a$ for all a, b in G, then it is said to be an* ***abelian group*** *or a* ***commutative group****. A "non-abelian group" or "non-commutative group" is one in which the group operation is not commutative. Under addition, $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ and $\mathbb{C}$ are abelian groups.*

Example 1.2. *($\mathbb{Z}$, +)*

Here, the identity is the additive identity, which is 0. Because $a + a^-1$ = a + (-a) = a-a = 0, we have a^-1 = a for every integer, a. Due to the fact that the sum of two numbers is always an integer, the integers under addition are finally closed. The integers with the addition operation ($\mathbb{Z}$, +) thus form a group. Due to the fact that a + b = b + a for any a, b in Z, this group is also abelian.

Example 1.3. *($\mathbb{Z}_5$, +)*

The group of integers modulo 5 falls as a group under the addition operation. If we add each number by adding the congruence class it belongs to, we see that $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Any two numbers added together and reduced mod 5 will always equal to 0, 1, 2, 3 or 4 and hence the group is closed. The identity is 0 just like any group under addition and every element has a unique inverse. So it is a group and eventually an abelian group. Its ***group table*** *is given below:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

1.3. ***FINITE GROUP*** *A group G is referred to as a* ***finite group*** *if it only has a finite number of elements; otherwise, it is referred to as an infinite group. The order of a group, O(G), is the total number of elements in a finite group G. In other words, if G has n elements, then O(G) = n.*

Example 1.4. *($\mathbb{Z}_5$, +) is a finite group of order 5 because it has elements 0, 1, 2, 3, and 4. But ($\mathbb{R}$, +) is an infinite group.*

1.2 Semigroups

1.4. ***SEMIGROUP*** *The set G is referred to as a semi-closed group or* ***semi group*** *if only the closure law and associative law are satisfied. Consequently, a semigroup is an algebraic structure made up of a set and an internal binary associative operation on it. Formally, associativity is defined as $(x.\ y).\ z = x.\ (y.\ z)$ for all x, y, and z in the semigroup. Without needing the existence of an identity element or inverses, semigroups can be thought of as a generalisation of groups or as a specific instance of magmas, where the operation is associative. Matrix multiplication is a well-known example of an operation* *that is associative but non-commutative, similar to how in groups or magmas the semigroup operation need not be commutative, so x.y need not equal to y.x. In the event that the semigroup operation is commutative, the semigroup is referred to as a commutative semigroup or, less frequently than in the similar case of groups, an abelian semigroup.*

A ***monoid*** *is an algebraic structure that is in the transition zone between semigroups and groups. It is a semigroup with an identity element and, as such, satisfies all but one of the group's axioms: the absence of inverses. In contrast to non-negative integers, which form a monoid, positive integers with addition form a commutative semigroup that is not a monoid. By simply including an identity element, a semigroup without identity can be converted into a monoid. As a result, rather than in group theory, monoids are investigated in the theory of semigroups.*

Example 1.5. *The set of positive integers under addition is a semigroup. (This becomes a monoid when 0 is added.)*

1.5. ***SUBGROUP*** *We say that a subset H of a group G is a* **subgroup** *of G if it is closed under the binary operation of G and if H is itself a group with the induced operation from G. G is the improper subgroup of G if G is a group. The remaining groupings are all proper subgroups. The trivial subgroup of G is the subgroup $\{e\}$. The remaining subgroups are all nontrivial.*

Example 1.6. *($\mathbb{Z}$, +) is a proper subgroup of ($\mathbb{R}$, +)*

The group table of Klein 4-group and all its subgroups and are given below:

Klein 4-group V is given by V=$\{e, a, b, c\}$ such that

$a.a{=}e \quad a.b{=}c$

$b.b{=}e \quad b.c{=}a$

$c.c{=}e \quad a.c{=}b$

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Hence subgroups of Klein 4-groups are

$H_1 = \{e,a,b,c\}$

$H_2 = \{e\}$

$H_3 = \{e,a\}$

$H_4 = \{e,b\}$

$H_5 = \{e,c\}$

1.6. *CYCLIC GROUP* *[2] We refer to a group G as a* ***cyclic group*** *if it has an element a that generates G when stated as $< a >= G$. In some circumstances, groups of infinite orders can be cyclic, and cyclic groups can have more than one generator. Examples will clearly demonstrate this.*

Example 1.7. *When we went back to ($\mathbb{Z}_10$, +), we noticed that $< 2 >$ only generated a subgroup of the group, not the entire group. Consider another element of this group. Observe that $< 7 >= \{7,4,1,8,5,2,9,6,3\} = \mathbb{Z}_10$ is obtained by continually adding 7 to itself and reducing mod 10.*

Example 1.8. *Remember that $< 1 >= \mathbb{Z}$. Therefore, since 1 is a generator of $\mathbb{Z}$. Hence*

($\mathbb{Z}$, +) must be cyclic. Take note that $\mathbb{Z}$ is of infinite order. As a result, groups with infinite order can truly be cyclic.

1.3 Rings

1.7. *RING* *[2]A set R is a **ring** if it has two binary operations addition) and multiplication and it satisfy the given three sets of axioms, called the ring axioms*

1. R under addition is an abelian group:

** (a + b) + c = a + (b + c) for all a, b, c in R (that is, + is associative).*

** a + b = b + a for all a, b in R (that is, + is commutative).*

** There is an element 0 in R such that a + 0 = a for all a in R (that is, 0 is the additive identity).*

** For each a in R there exists $-a$ in R such that a + $(-a)$ = 0 (that is, -a is the additive inverse of a).*

2. Multiplication is associative

3. Multiplication is distributive with respect to addition. That is for all a,b,c in R,

** a · (b + c) = (a · b) + (a · c) (left distributive law).*

** (b + c) · a = (b · a) + (c · a) (right distributive law).*

Example 1.9. $<Z, +, .>$ *is a ring.*

Example 1.10. *The set of natural numbers with the usual operations is not a ring, because it is not even a group as all the elements are not invertible with respect to addition .In order to enlarge it to a ring, include negative numbers to produce the ring of integers.*

1.8. ***COMMUTATIVE RING*** *Ring multiplication does not have to be commutative; ab need not always equal ba. But ring addition is commutative.* ***Commutative rings****, such as the ring of integers, are rings that also meet commutativity for multiplication.*

Example 1.11. *2 $\mathbb{Z}$ with usual addition and multiplication is a commutative ring.*

1.9. ***FIELD*** *A division ring (skew field) is a ring such that every non-zero element is a unit(has multiplicative inverse). A commutative division ring is a* ***field*** *and a non-commutative division ring is a strictly skew field.*

Example 1.12. *The set of rational numbers is a field since every non-zero element has a multiplicative inverse.*

1.10. ***SUBRING*** *A subring of a ring is defined as the subset of the ring that is a ring under induced operations from the whole ring.*

Example 1.13. *The ring of integers is a subring of the field of real numbers.*

1.4 Semirings

1.11. ***SEMIRINGS*** *A non-empty set S combined with the two binary operations + and . , such that the two distributive laws are satisfied, constitutes a* ***semiring*** *(S, +, .). That is a semiring (S, +,.) is a non-empty set S along with two binary operations, + and . where*

1. (S, +) is a commutative monoid with identity element 0

2. (S, .) is a monoid with identity element 1

3. a. (b + c) = a. b + a .c and (b + c). a = b. a + c. a for all a,b,c in S

Example 1.14. *The set of all positive integers with usual addition and multiplication is a semiring.*

1.12. ***COMMUTATIVE SEMIRINGS*** *[1] If (S, +) is a commutative semigroup, then the semiring (S, +, .) is said to be additively commutative. If (S, .) is a commutative semigroup, then a semiring (S, +, .) is said to be multiplicatively commutative. If (S, +) and (S, .) are both commutative, then it is said to be* ***commutative****.*

Example 1.15. *The set of natural numbers including zero under ordinary addition and multiplication is a commutative semiring.*

If the semiring (S, +, .) has a '0' element in S such that $\boldsymbol{x + 0 = x = 0 + x}$ *for all x in S, then it is said to be a semiring with zero. If there is 1 in S such that* $\boldsymbol{1 \,.\, x = x = x \,.\, 1}$*, for all x in S, then a semiring (S, +, .) is said to have an identity element 1.*

1.13. ***SUBSEMIRING*** *[1] Let a semiring be (S, +, .). Any nonempty subset A of S that contains '0' and '1' and is closed under the operations '+' and '.' is referred to as a* ***subsemiring****.*

Example 1.16. $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ *is the subsemiring of the set of all matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *with integer entries.*

Chapter 2

DERIVATIONS ON SEMIRINGS

2.1 Derivations on rings

[1]Suppose R is an associative ring. Then a mapping $d : R \to R$ is called a ***derivation*** *if*

i. $d(x + y) = d(x) + d(y)$

ii. $d(xy) = d(x)\, y + x\, d(y)\ \forall\ x, y$ *in* R

Example 2.1. *Let R be a ring of 2×2 matrices.*

Define $d{:}R \Rightarrow R$ by

$$d\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} 0 & -q \\ r & 0 \end{pmatrix}$$

Then d is a nonzero derivation on R since we have

$$d\left(\begin{pmatrix} x & y \\ z & w \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = d\begin{pmatrix} x+a & y+b \\ z+c & w+d \end{pmatrix} = \begin{pmatrix} 0 & -(y+b) \\ z+c & 0 \end{pmatrix}$$

$$d\begin{pmatrix} x & y \\ z & w \end{pmatrix} + d\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -y \\ z & 0 \end{pmatrix} + \begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & -(y+b) \\ z+c & 0 \end{pmatrix}$$

2.1. *INNER DERIVATION* *[1]In specifically, if $a \in R$ is fixed, the mapping $I_a : R \Rightarrow R$ provided by $I_a(x) = [x, a] = xa - ax$ is a derivation that is referred to as an **inner derivation**.*

Example 2.2. *We can start with the ring of square matrices over a field, or $M_n(F)$. Here n is the size of the matrices and F is the field. The Leibniz rule is satisfied by a linear map $D : M_n(F) \Rightarrow M_n(F)$, which is a derivation on this matrix ring given by:*

D(AB)=D(A) B+A D(B)

A derivation that may be "generated" by a fixed matrix X using the following formula is referred to as an inner derivation in this instance:

$$D_X(A) = XA - AX$$

Where A is any $M_n(F)$ matrix. Because it is defined in terms of the commutator operation $[X, A] = XA - AX$, which gauges how much X fails to commute with A, this is known as an inner derivation.

2.2. *GENERALIZED DERIVATION* *[1] If F (xy) = F (x) y + x d(y) for all x, y in R and F(x+y)= F(x) + F(y), then the additive function $F : R \Rightarrow R$ is known as a **generalized derivation** and has an associated derivation d on R.*

Example 2.3. *Given $R = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ where x,y,z in $\mathbb{Z}$.*

Suppose m to be a fixed non zero element in $\mathbb{Z}$ and define $F : R \Rightarrow R$ by

$$F\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & mx + mz \\ 0 & 0 \end{pmatrix}$$

Here we have F to be a generalized derivation having associated derivation d such that,

$$d\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & mx - mz \\ 0 & 0 \end{pmatrix}$$

2.2 Derivations on semirings

[1] Suppose (S, +, ·) be a semiring. A ***derivation on S*** *is a map $D : S \to S$ satisfying the following conditions*

1. D(x + y) = D(x) + D(y), for all x, y in S.

2. D(xy) = D(x)y + xD(y) for all x, y in S.

Example 2.4. *For a semiring S, the set S[x] of polynomials under usual addition and multiplication of polynomials is a semiring. Taking $f(x) = a_0 + a_1x + ... + a_nx^n$ from S[x] and defining the map D: S $\Rightarrow$ S by*

D(f(x)) $= a_1 + 2a_2x + ...na_nx^{(n-1)}$

gives us D to be a derivation on S[x].

Lemma 2.1. *[1] On an additively commutative semiring (S, +, .), sum of two derivations is again a derivation.*

Proof. Let the additively commutative semiring S has the derivations D_1 and D_2.

Then,

$(D_1 + D_2)$(a + b)

$= D_1(a + b) + D_2(a + b)$

$=D_1(a) + D_1(b) + D_2(a) + D_2(b)$

$=(D_1 + D_2)$(a) + $((D_1 + D_2)($ b)

Also,

$(D_1 + D_2)$(ab)

$= D_1(ab) + D_2(ab)$

$= D_1(a)b + aD_1(b) + D_2(a)b + aD_2(b)$

$=D_1(a)b + D_2(a)b + aD_1(b) + aD_2(b)$

$=(D_1(a) + D_2(a))b + a(D_1(b) + D_2(b))$

$=(D_1 + D_2)(a)b + a(D_1 + D_2)(b)$

■

Lemma 2.2. *[1] Product of two derivations in general need not be a derivation.*

Proof. Additivity can be proved easily here. But,

$D_1.D_2$(ab) $=D_1(D_2$(ab))

$=D_1(D_2$(a)b + aD_2(b))

$=D_1(D_2$(a)b) + $D_1(aD_2$(b))

$=D_1(D_2$(a))b + D_2(a) $D_1(b)$ + D_1(a) $D_2(b)$ + a$D_1(D_2(b))$

$=(D_1.D_2$(a))b + a$(D_1.D_2)(b) + D_2$(a) $D_1(b)$ + D_1(a) $D_2(b)$

$\neq(D_1.D_2)$(a)b + a$(D_1.D_2)(b)$

■

Chapter 3

SEMIRINGS AND GRAPHS

3.1 Construction of semirings

Here we are going to deal with a new semiring structure known as the semiring of graphs, that is semirings made on graphs. This approach will help us to solve artificial network problems by fusing algebraic theory and graph theory in view of semirings. First of all we will introduce $\cup$, $\cap$, ∇ *called union, intersection and join, which are the algebraic operations of graphs. Then we have the structures* $(S,\cup,\cap)$ *and* $(S,\cup,\nabla)$ *to be the semirings where S is given as a set of simple undirected graphs.*

A semiring is typically described as a non-empty set S plus two binary operations, addition and multiplication, indicated by (S, +, .), where addition and multiplication are coupled by distributivity and (S, +) and (S, .), respectively, are monoid and semigroup. Here, we limit ourselves to Vandiver's formal definition of semirings, which omits the necessity of neutral elements and the absorption feature. For our purposes, loops are ignored and parallel edges linking any two vertices are merged. The set of all simple undirected graphs will henceforth be referred to as S.

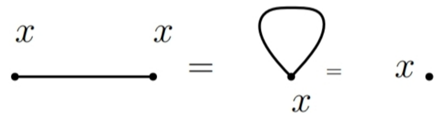


Figure 3.1: A self loop to a singleton vertex

The graph $G=G_1 \cup G_2=(V_1 \cup V_2, E_1 \cup E_2)$ *is defined as the union of two graphs,* $G_1=(V_1,E_1)$ *and* $G_2=(V_2,E_2)$*. The join of two graphs G and H results in a graph that is created by taking the union of edge sets of both these graphs and linking each vertex of G to each vertex of H, while ignoring self-loops and multiple edges. It is represented by the notation* $G \nabla H = (V(G) \cup V(H), E(G) \cup E(H) \cup (u, v) : u \in V(G)$ *and* $v \in V(H)$*excluding*$(aa: a \in V(G) \cap V(H)$.

Now we have another binary operation called intersection, which is indicated by

$G=G_1 \cap G_2=(V_1 \cap V_2, E_1 \cap E_2)$

It signifies the merging of similar vertices and edges of both the given graphs. On considering the set of undirected simple graphs S with the two binary operations graph union $\cup$ *and join* ∇*, if the combining of the graph using these operations arise any self loops then they are ignored. For any* G_1*,* G_2 *in S,*

$(G_1 \nabla G_2) = G_2 = (G_1 \cup G_2)$

or

$(G_1 \nabla G_2) = G_1 = (G_1 \cup G_2)$

where G_1 *is taken as the subgraph of* G_2 *or* G_2 *as the subgraph of* G_1*. This gives*

$(G_1 \nabla G_2) = (G_1 \cup G_2)$ *for all* G_1*,* G_2 *in S.*

On the contrary, assume that they are not subgraphs of each other. Then we must have the number of edges of $G_1 \nabla G_2$ *greater than that of* $G_1 \cup G_2$. *This gives* $(G_1 \nabla G_2) \neq (G_1 \cup G_2)$ *thus giving a contradiction. Hence we can say that for a semiring* $(S, \cup, \nabla)$, $(G_1 \nabla G_2) = (G_1 \cup G_2)$ *iff either of the given two graphs must be a subgraph of the other.*

Given three graphs G_1, G_2 *and* G_3.

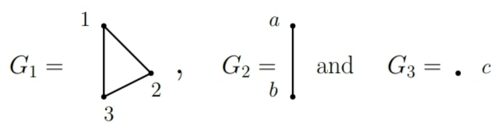


Figure 3.2: Illustrative graphs

Then we can see that these graphs satisfy some of the algebraic axioms which are given below.

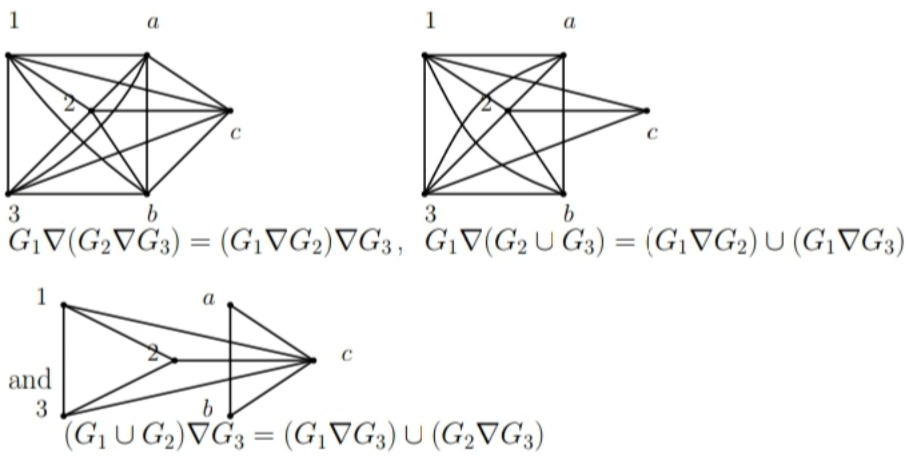


Figure 3.3: First one showing associativity of ∇, second and third showing distributivity of ∇ over $\cup$

Theorem 3.1. *[3] If S is the set of all graphs, then (S,$\cup$,∇) is a semiring.*

Proof. First of all, we need to prove that (S, $\cup$) is a semigroup. If we take two graphs G_1, G_2 from S, we have $G_1\cup$G$_2$ also in S. Let G_3 also belongs to S. For a vertex u taken from $G_1\cup$(G$_2\cup$G$_3$),

u $\in$ V($G_1\cup$(G$_2\cup$G$_3$))

$\Longleftrightarrow u\in$ V(G_1) $\cup$(V(G$_2$) $\cup V$(G$_3$))

$\Longleftrightarrow u\in$ V(G_1) or (u $\in$ V(G_2) or u $\in$ V(G_3))

$\Longleftrightarrow$ ($u\in$ V(G_1) or u $\in$ V(G_2)) or u $\in$ V(G_3)

$\Longleftrightarrow u\in$ (V(G_1) $\cup V$(G$_2$)) $\cup V$(G$_3$)

$\Longleftarrow u\in$ V(($G_1\cup$G$_2$)$\cup$G$_3$)

Thus we can conclude that V($G_1\cup$(G$_2\cup$G$_3$)) = V(($G_1\cup$G$_2$)$\cup$G$_3$). Vice-versa can also be proved. Hence we proved $\cup$) is a semigroup. Now similarly we can prove that $G_1\nabla$(G$_2\nabla$G$_3$) = ($G_1\nabla$G$_2$)∇G$_3$. Finally we prove that ∇ distributes over $\cup$. That is we get $G_1\nabla$(G$_2\cup$G$_3$) = ($G_1\nabla$G$_2$)$\cup$($G_1\nabla$G$_3$). Hence we can conclude that (S,$\cup$,∇) is a semiring.

■

3.2 Semirings of weighted graphs

On the above we discussed only about algebraic structures of graphs with 2-tuppled elements(edges and vertices). Now we extend it to form algebraic structures of graphs with 3-tuppled elements by adding the weight function of each edge. Here we merge the parallel lines and treat it as a single path thus getting a shortest path. We can denote the set of all weighted graphs S as (V,E,W) with V as set of vertices, E as set of edges and

W the corresponding weights. Hence we denote an empty graph as $(V\phi, E\phi, W\phi)$ *with empty set of vertices, empty set of edges and corresponding weights. Similar is the case of* $(V\infty, E\infty, W\infty)$ *with infinte number of vertices and edges. Then we define the two binary operations* $\bigoplus$ *and* $\bigotimes$ *on S as*

$$(V_1, E_1, W_1) \bigoplus (V_2, E_2, W_2) = \begin{matrix} (V_1, E_1, W_1) & \text{if } (V_1, E_1, W_1) \neq (V\infty, E\infty, W\infty) \\ (V_2, E_2, W_2) & \text{otherwise} \end{matrix}$$

where (V_1, E_1, W_1), (V_2, E_2, W_2) *are in S.*

Also,

$(V_1, E_1, W_1) \bigotimes (V_2, E_2, W_2) = (V_1 \bigotimes V_2,\ E_1 \bigotimes E_2,\ W_1 \bigotimes W_2)$.

Here $V_1 \bigotimes V_2$ *considered as the union of* V_1 *and* V_2*, while* $E_1 \bigotimes E_2$ *have those edges either present in* E_1 *or* E_2 *or those drawn by connecting each vertex of* v_1 *to every vertex of* V_2 *having edge weight 1. By doing so, we are able to merge the multiple edges and hence the weight of the resultant edge will be minimum.* $W_1 \bigotimes W_2$ *gives us the required edge weights in the resulting graph.*

Note 3.1. *[3] The set of all weighted graphs S together with the binary operations* $\bigoplus$ *and* $\bigotimes$ *is a semiring.*

3.3 Algorithm to get the shortest path

Consider G to be the graph required with node labels taken from an ordered idempotent semiring $(R, \bigoplus, \bigotimes)$ *with* $\bigoplus$ *and* $\bigotimes$ *as maximum and minimum operations. The reason behind the selection of nodes from an ordered idempotent semiring is to get the optimal* *path.*

1. Take the source vertex s and the target vertex d of the given network G. Consider all sequences of edges joining this s and d. Let these sequences be E, E_2*,....*E_n*.*

2. From these sequences of edges, remove those edges with source or destination vertex and then take the join of the edges left to obtain the graphs p_1*,* p_2*,....*p_n*.*

3. Consider the union of the deleted edges and let it be $p^{'}$*.*

4. Get the new graph $G^{'} = p_1 \cup p_2 \cup ..... \cup p_n \cup p^{'}$*. Now each edge (u,v) of this graph is labelled with (u* $\bigoplus$ *v) or (u* $\bigotimes$ *v) according to the problem.*

5. Next we use Dijkstra's algorithm to find the shortest path of G' as it is the simplest method to find the shortest path in a weighted graph.

For the network given below, we are going to find shortest path from source vertex 0 to target vertex 6.

Sequences of edges joining 0 and 6 are given by

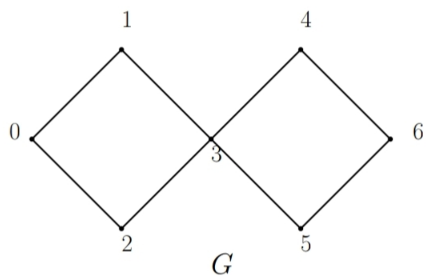


Figure 3.4: G

E_1 *= [(0,1)(1,3)(3,4)(4,6)]*

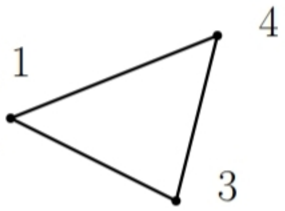
E_2 = *[(0,1)(1,3)(3,5)(5,6)]*

E_3 = *[(0,2)(2,3)(3,5)(5,6)]*

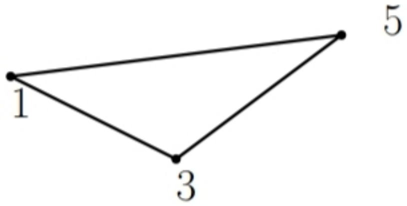
E_4 = *[(0,2)(2,3)(3,4)(4,6)]*

From each sequence, remove edges with source or target vertex. Then we get

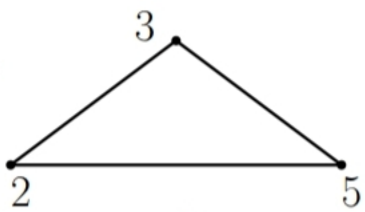
$$p_1 = (1,2)\nabla(3,4) =$$



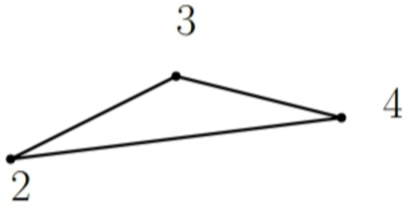
$$p_2 = (1,3)\nabla(3,5) =$$



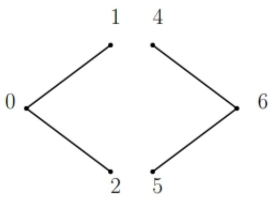
$$p_3 = (2,3)\nabla(3,5) =$$



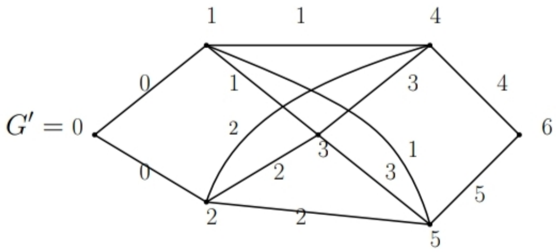
$$p_4 = (2,3)\nabla(3,4) =$$



Then union of the deleted edges is given by p'. Next we construct the optimal graph G' by *adding the edges (1,4),(2,5),(1,5),(2,4) to G.*

$p' = (0,1) \cup (0,2) \cup (4,6) \cup (5,6) =$ 

Therefore,



Now the shortest path from 0 to 6 is given by Dijkstra's algorithm.

	0	1	2	3	4	5	6
0	$\boxed{0}$	∞	∞	∞	∞	∞	∞
1		$\boxed{0}$	0	∞	∞	∞	∞
2			$\boxed{0}$	1	1	1	∞
3				$\boxed{1}$	1	1	∞
4					$\boxed{1}$	1	∞
5						$\boxed{1}$	5
6							$\boxed{5}$

The table shows the minimum weight of the path from 0 to 6 as 5 and the path as 0-1-4-6, *by back tracking in the table.*

Chapter 4

Homomorphisms and derivations

4.1 Group Homomorphism

If we are given by two groups G and G', there are maps that relate the group structure of one of these to the other. In such a case if the structural properties of G is known, we can get the information about G' also, because it is structurally just a copy of G.

4.1. ***HOMOMORPHISM***[2] *A map ϕ from a group G to a group G' is said to be a homomorphism if it holds the given property $\forall$ a,b in G.*
$\phi(ab) = \phi(a)\ \phi(b)$

suppose if we take any group G and G', there will be always atleast one homomorphism ϕ: G $\Rightarrow$ G'. It is known as ***trivial homomorphism*** *which is given by $\phi(g)$ = e' for all g in G.*
For a group homomorphism ϕ from G to G', if G is taken as an abelian group then G' will also be abelian.
For a homomorphism ϕ_c: F $\Rightarrow$ R, where F is the additive group of all functions mapping

R into R , R be the additive group of real numbers and c be any real number with $\phi_c(f) = f(c)$ *for f in F, we have*

$\Phi_c(f+g) = (f + g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$

This is known as the ***evaluation homomorphism****.*

4.2. ***PROPERTIES OF HOMOMORPHISMS****[2]*

Let ϕ*:* $G \Rightarrow G'$ *be a homomorphism, where G and G' are groups.*

1. $\phi(e) = e'$ *is the identity element in G', if e is the identity element of G*

2. For $b \in G$*,* $\Phi(b^-1) = \phi(b)^-1$

3. $\phi[K]$ *is a subgraph of G', if K is a subgroup of G.*

4. $\phi^-1[H']$ *is a subgroup of G, if H' is a subgroup of G'.*

Example 4.1. $\phi : \mathbb{Z} \Rightarrow \mathbb{R}$ *given by* $\phi(n)=(n)$ *is a homorphism under addition.*

4.2 Ring Homomorphism

Since homomorphism is defined as a structure relating map, in the case of rings it must relate additive structure and multiplicative structure of rings.

4.3. ***HOMOMORPHISM****[2] A map* ϕ *of a ring R into a ring R' is a homomorphism if*

$\phi(a+b) = \phi(a) + \phi(b)$

and

$\phi(ab) = \phi(a)\phi(b)$

for all elements a,b in R.

Example 4.2. *(Projection homomorphism)[2] For rings R_1,R_2,...,R_n, we have the map π_i from $R_1 \times R_2 \times ... \times R_n$ to R_i where $\pi_i(r_1,r_2,...,r_n)$=r_i is a homomorphism projected to the ith component.*

4.4. *PROPERTIES OF HOMOMORPHISM*[2] *Let ϕ: $R \Rightarrow R'$ be a homomorphism, where R and R' are rings.Then*

1. $\phi(0) = 0'$ is the additive identity element in R', if 0 is the additive identity element of R.

2. For $b \in R$, $\phi(-b)$=- $\phi(b)$

3. $\phi[K]$ is a subring of R', if K is a subring of R.

4. $\phi^{-}1[H']$ is a subring of R, if H' is a subring of R'.

5. $\phi(1)$ is the unity of $\phi[R]$, if 1 is the unity of R.

4.3 SEMIRING HOMOMORPHISM

4.5. *[3] Let (S,+,.,0,1) and (S',$\bigoplus$,$\bigotimes$,0',1') be two semirings. Then the map f: S' is said to be a semiring homomorphism if for all a,b in S,*

$f(a+b) = f(a) \bigoplus f(b)$,

$f(a.b) = f(a) \bigotimes f(b)$,

$f(0) = 0'$ and

$f(1) = 1'$

Example 4.3. *Let $P(Z_0)$ be taken as the power set of the non negative integers Z_O. Then $(Z_0,+,.,0,1)$and$(P(Z_0),\cup,\cap,\phi,(Z_0))$ are semirings with operations usual addition and multiplication on (Z_0) and usual set union and intersection on $P(Z_0)$.*
Then we have the mapping ϕ: $Z_0 \Rightarrow P(Z_0)$ by $\phi(n) = [n] = \ 0, 1, 2, ..., n-1\}$ is a semiring homomorphism.

4.4 Relation between homomorphisms and derivations on semirings

Homomorphisms and derivations have a link in semiring theory. A semiring is a set that has two binary operations—addition (+) and multiplication (.)—and meets specific criteria.
A function that preserves the structure of the semirings, including the addition and multiplication operations, is called a homomorphism between two semirings. On the other hand, a function that satisfies a property comparable to the calculus product rule is a derivation on a semiring.
A derivation is specifically a function D from a semiring R to itself such that the following is true for any elements a and b in R.
1. (Derivation respects addition) D(a+b) = D(a) + D(b)
2. D(a.b) = D(a).b + a.D(b) (respecting multiplication in the derivation)
Any homomorphism between two semirings also induces a derivation, which is how homomorphisms and derivations are related.
For example, let ϕ be the homomorphism from semiring R to semiring S, then we have

the function D(a)= ϕ*(a) -* ϕ*(0) to be the derivation on R.*

Conclusion

Semirings have wide applications in various fields such as mathematics, computer science and engineering. They are used to model graph algorithms like that of Dijikstra's algorithm we done in this paper. They also find applications in cryptography, optimization problems , network flow analysis, signal processing and automata theory. Through this paper we could study about semirings, their derivations, application in graph theory and relation between homomorphisms and derivations on semirings.

Bibliography

[1] M Chandramouleeswaran and V Thiruveni. On derivations of semirings. Advances in algebra*, 3(1):123–131, 2010.*

[2] John B Fraleigh. A first course in abstract algebra*. Pearson Education India, 2003.*

[3] Saifur Rahman and Gete Umbrey. Semirings of graphs: homomorphisms and applications in network problems. Proyecciones (Antofagasta)*, 41(6):1273–1296, 2022.*