UNIVERSITY OF BANJA LUKA
FACULTY OF NATURAL SCIENCES AND MATHEMATICS

IVAN VANJA BOROJA

COMPRESSION OF THE COMMUTING GRAPH OF RINGS AND OTHER ALGEBRAIC STRUCTURES

DOCTORAL DISSERTATION

BANJA LUKA, 2025.

UNIVERSITY OF BANJA LUKA
FACULTY OF NATURAL SCIENCES AND MATHEMATICS

IVAN VANJA BOROJA

COMPRESSION OF THE COMMUTING GRAPH OF RINGS AND OTHER ALGEBRAIC STRUCTURES

DOCTORAL DISSERTATION

BANJA LUKA, 2025.

UNIVERZITET U BANJOJ LUCI
PRIRODNO-MATEMATIČKI FAKULTET

IVAN VANJA BOROJA

KOMPRESIJA GRAFA KOMUTATIVNOSTI PRSTENA I DRUGIH ALGEBARSKIH STRUKTURA

DOKTORSKA DISERTACIJA

BANJA LUKA, 2025.

Supervisor: Nik Stopar, Ph.D., assistant professor at the Faculty of Civil and Geodetic Engineering, University of Ljubljana
Co-supervisor: Duško Bogdanić, Ph.D., full professor at the Faculty natural Sciences and Mathematics, University of Banja Luka

Title: Compressed commuting graph of rings and other algebraic structures

Abstract

In this thesis we investigate the recently introduced compressed commuting graph $\Lambda^1(R)$ of a unital ring R. This is a graph whose vertices are equivalence classes of elements of R according to the relation $\sim$ which is defined as $a \sim b$ if and only if a and b generate the same unital subring. Two vertices are connected by an edge if and only if their representatives commute. This graph can be seen as a compression of the regular commuting graph $\Gamma(R)$. We prove in the thesis that for matrix algebras over finite fields this compression is the best possible compression that induces a functor from the category of unital rings to the category of graphs. We also discuss some properties of this graph, for example, the graph gives information about the set of unital subrings of R generated by one element. This view was applied in our result characterizing infinite unital rings with only finitely many unital subrings.

In our recent article we were able to completely describe the graph $\Lambda^1(\mathcal{M}_2(\mathbb{F}))$ for a finite field $\mathbb{F}$. The main contribution of this thesis is the complete description of the graph $\Lambda^1(\mathcal{M}_3(\mathbb{F}))$ for a prime field $\mathbb{F} = GF(p)$. To achieve this goal we combined methods from field theory, projective geometry and combinatorics. We first describe the set of vertices, relying on the Jordan form of matrices, and then determine the structure of the neighborhood of each vertex. The core part of the graph is then described using a bijective correspondence with a point-line pairs in the projective plane over $GF(p)$. In addition, we also give a short algorithm that can be used to construct $\Lambda^1(\mathcal{M}_3(GF(p)))$. As a consequence of our result we are also able to describe the graph $\Gamma(\mathcal{M}_3(GF(p))$ using the so-called "blow-up" process. The description of this graph was an open problem for several years.

Keywords: Commuting graph, compressed commuting graph, matrix ring, finite field

Scientific area: Natural Sciences

Scientific field: Mathematics

CERIF classification code: P120

Mentor: dr Nik Stopar, docent na Građevinsko-geodetskom fakultetu Univerziteta u Ljubljani
Komentor: dr Duško Bogdanić, redovni profesor na Prirodno-matematičkom fakultetu, Univerzitet u Banjoj Luci

Naslov: Kompresovani graf komutativnosti prstena i drugih algebarskih struktura

Rezime

U ovoj tezi istražujemo nedavno predstavljeni kompresovani graf komutativnosti $\Lambda^1(R)$ jediničnog prstena R. Ovo je graf čiji su vrhovi klase ekvivalencije elemenata prstena R u odnosu na relaciju $\sim$ koja je definisana sa $a \sim b$ ako i samo ako a i b generišu isti jedinični podprsten. Pri tome, dva čvora su povezana granom ako i samo ako njihovi predstavnici komutiraju. Ovaj graf se može vidjeti kao kompresija uobičajenog grafa komutativnosti $\Gamma(R)$. U tezi dokazujemo da je, za matrične algebre nad konačnim poljima, ova kompresija najbolja moguća kompresija koja indukuje funktor iz kategorije jediničnih prstena u kategoriju grafova. Takodje, raspravljamo o nekim svojstvima ovog grafa, na primjer, graf daje informacije o skupu jediničnih podprstena R generisanih jednim elementom. Ovakav pristup je primijenjen u našem rezultatu koji karakteriše beskonačne jedinične prstenove sa konačnim brojem jediničnih podprstena.

U našem nedavno objavljenom članku uspjeli smo u potpunosti opisati graf $\Lambda^1(\mathcal{M}_2(\mathbb{F}))$ za konačno polje $\mathbb{F}$. Glavni doprinos ove teze je potpuni opis grafa $\Lambda^1(\mathcal{M}_3(\mathbb{F}))$ za prosto polje $\mathbb{F} = GF(p)$. Da bismo postigli ovaj cilj, kombinovali smo metode iz teorije polja, projektivne geometrije i kombinatorike. Prvo opisujemo skup vrhova, oslanjajući se na Žordanovu formu matrice, a zatim određujemo strukturu susjedstva svakog vrha. Glavni dio grafa se zatim opisuje korištenjem bijektivne korespondencije s parovima tačka-linija u projektivnoj ravni nad poljem $GF(p)$. Osim toga, dajemo i kratki algoritam za konstrukciju $\Lambda^1(\mathcal{M}_3(GF(p)))$. Kao posljedica našeg rezultata, takođe smo u mogućnosti opisati graf $\Gamma(\mathcal{M}_3(GF(p))$ korištenjem takozvanog procesa "eksplozije". Opis ovog grafa bio je otvoren problem nekoliko godina.

Ključni pojmovi: Graf komutativnosti, kompresovani graf komutativnosti, prsten matrica, konačna polja

Naučna oblast: Prirodne nauke

Naučno polje: Matematika

Klasifikacioni kod prema CERIF-u šifrarniku: P120

Contents

1 Introduction **1**

2 Preliminaries **5**

3 Compressed commuting graph of a unital ring **15**

4 Compressed commuting graph of $\mathcal{M}_2(GF(p))$ **19**

5 Vertex set of $\Lambda^1(\mathcal{M}_3(GF(p)))$ **29**

6 Neighborhoods of vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$ **47**

7 Subgraph induced on $V_{(B)} \cup V_{(E)}$ **61**

7.1 Projective plane over $GF(p)$ and its incidence matrix 61

7.2 Bijection between $V_{(B)} \cup V_{(E)}$ and $\mathscr{P} \times \mathscr{L}$ 64

7.3 Geometrical interpretation of edges 66

8 Description of $\Lambda^1(\mathcal{M}_3(GF(p)))$ **69**

8.1 Properties of $\Lambda^1(\mathcal{M}_3(GF(p)))$ 69

8.2 Construction of $\Lambda^1(\mathcal{M}_3(GF(p)))$ 72

9 Commuting graph of $\mathcal{M}_3(GF(p))$ **73**

Bibliography **74**

Chapter 1

Introduction

One of the most important notions in algebra is the notion of commutativity. Given an algebraic structure A, equipped with an operation of multiplication, two elements a and b from A *commute* if and only if $ab = ba$. It is said that an algebraic structure A is *commutative* if every two elements from A commute. If the structure A is not commutative, it is important to investigate the properties of the relation of commutativity in A. There are various approaches to this problem but one of the most recent ones is to visualize the relation of commutativity using the graph, the so called *commuting graph*, where vertices correspond to the non-central elements of the structure and the edges describe commutativity. This is particularly interesting for finite structures, since we obtain finite graphs.

To the best of our knowledge, this approach was first developed for groups in [15] as an attempt towards the classification of finite simple groups. Since then, the commuting graph of finite groups have been investigated by several authors. In [28] the authors prove that the isomorphism problem, which asks whether two groups with isomorphic commuting graphs are themselves isomorphic, has a positive answer for many simple groups. The properties of the commuting graph of symmetric and alternating groups, in particular, its diameter, was considered in [29], while the diameter of the commuting graph of a general finite group was discussed in [36]. Recently, some interesting connections between the structure of the group and the structure of its commuting graph were discovered in [34]. The definition of the commuting graph was later extended to several other algebraic structures. For rings, the commuting graph was introduced in [2] where the authors determined the minimum and maximum degree and the clique number of the graph of the ring of matrices over a finite field. They also discuss the isomorphism problem for this graph. The commuting graph of a ring has attracted a lot of attention since its introduction. The research focuses mainly on the properties of this graph such as the connectedness and diameter, as well as the isomorphism problem for this graph, see for example [1, 35, 19, 24]. Furthermore, the commuting graph was also considered for bounded linear operators on a Hilbert space, see [5]. In [32] it was shown that the commuting graph of the Banach algebra of bounded linear operators on a complex Hilbert space determines the dimension of the Hilbert space. Some results can be found on commuting graph of semigroups

[9], Lie algebras [40], etc.

In this thesis we will be mostly interested in the investigation of the relation of commutativity in unital rings, in particular, rings of matrices over finite fields. The commuting graph of the ring was introduced in [2]. Given a ring R, the commuting graph $\Gamma(R)$ is a simple graph whose vertices are non-central elements of the ring R and two different elements a, b from the ring are connected by an edge if and only if $ab = ba$. Over the past two decades the commuting graph of a ring was investigated by many researchers who studied the connectedness [1, 20], diameter and girth [4, 21, 39], clique number [2], etc. Some authors also investigate the complement of this graph [25].

The main motivation for considering the commuting graph of a ring is to be able to use graph theoretical tools to investigate and describe the structure and properties of the ring. This immediately opens an important question whether the graph $\Gamma(R)$ uniquely determines the ring R. In particular, if $\Gamma(R_1) \cong \Gamma(R_2)$ does it follow that $R_1 \cong R_2$? This is known as the *isomorphism problem.* A particularly important case of this problem is the case when $R_1 = \mathcal{M}_n(\mathbb{F})$ is the ring of matrices over a finite field $\mathbb{F}$. In this case the isomorphism problem has a positive answer when $n = 2$ and $n = 3$ as shown in [35] and [24]. Also, when $n = 2^k 3^l$ with $k \geq 1$ a positive answer is given in [23]. For other values for n it is still an open problem. Another important problem is the problem of automorphism which asks whether any automorphism of the graph $\Gamma(R)$ is induced by an automorphism of a ring R, see for example [41].

There are several other types of graphs which help us in understanding the structure and various properties of rings. Examples of such graphs are the zero-divisor graph [8, 38], the total graph [6] and inclusion ideal graph [3]. Let us look at the zero-divisor graph more closely, in order to explain the motivation for the present thesis. The zero-divisor graph of a ring R is a simple graph whose vertices are nonzero zero-divisors of R where two distinct zero-divisors a and b are connected by a (directed) edge if and only if $ab = 0$, see [8, 38]. For certain rings this graph can have a lot of vertices and edges which makes it hard to visualize. In an attempt to make the graph smaller and thus more manageable Mulay introduced the graph of equivalence classes of zero-divisors of a commutative ring, see paper [37]. This graph was later called the *compressed zero-divisor graph* by Anderson and LaGrange [7]. Mulay identified the elements that are indistinguishable in the zero-divisor graph, i.e., have the same annihilator, and compressed them into one vertex. Although this compression significantly reduces the size of the vertex set of the graph it lacks certain favorable properties. In particular, it does not behave well when homomorphisms of rings are considered. To resolve this issue, a new type of compression was introduced in [16, 17], which was used to define new compressed zero divisor graph $\Theta(R)$. The compression was based on different relation of equivalence, that identified the elements which generate the same one-sided ideals. The benefit of this new approach is that the creation of the compressed zero-divisor graph can be extended to a functor Θ from the category of rings and ring homomorphisms to the category of simple graphs with loops and graph homomorphisms. Furthermore, this means that the graph $\Theta(R)$ better captures the structural properties of the ring R in the sense that there is a nicer connection between the structure of R and the structure of $\Theta(R)$, see [16, 17] for more details. It was even shown in the same papers that the chosen compression is the best possible, i.e., underlying relation of equivalence is the coarsest relation of equivalence that still induces a functor, see [17, Proposition 2.3].

The starting point for this thesis was the question of whether this categorical approach can be adapted to the setting of the commuting graph. We want to introduce *the compressed commuting graph* $\Lambda^1(R)$ as a compression of the commuting graph $\Gamma(R)$. Given a unital ring R, the vertices of $\Lambda^1(R)$ are equivalence classes of elements of R, with respect to the equivalence relation defined by $a \sim b$ if and only if elements a and b generate the same unital subring of R. Two vertices are adjacent if their respective representatives commute in R (see Definition 3.3 for details). Note that we do not exclude the center of R from the graph as in the classical commuting graph $\Gamma(R)$. It is shown in the thesis that compression based on this relation of equivalence induces a functor from the category of unital rings and unital ring homomorphisms to the category of undirected simple graphs with added loops and graph homomorphisms. The graph $\Lambda^1(R)$ has significantly smaller number of vertices than $\Gamma(R)$. Additionally, every vertex of $\Lambda^1(R)$ corresponds to a unital subring of R generated by one element, so $\Lambda^1(R)$ yields information about the set of such subrings of R.

The main goal of this thesis is the complete description of the compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$. As evident from the discussion above this graph has great potential to be used for further investigation of the ring of matrices. For example, having an explicit description of the graph may help us solve the isomorphism problem for this graph in the future.

One of the primary difficulties was to describe the set of vertices. We tackle this problem by considering cases based on the Jordan form of a matrix. We show that matrices that are compressed into a single vertex always have the same Jordan structure with possible different eigenvalues. That allows us to describe the vertices case by case, which makes the process of describing compressed commuting graph more manageable. After the set of vertices is determined, we carefully investigate the structure of the neighborhood of vertices in each case, determining how many vertices in the neighborhood are of a certain type. It turns out that this is crucial for detecting that some parts of the graph are easy to describe while some parts are not. The core part of the graph consists of vertices obtained by compression of non-derogatory matrices. We describe this part of the graph by establishing a bijective correspondence between the set of its vertices and the set of point-line pairs in the projective plain over $GF(p)$. Using this correspondence, we then describe the edges between the vertices of this part of the graph using the geometry of point-line pairs.

The rest of the graph is obtained by attaching vertices from other cases, respecting the neighborhoods of vertices, determined in the previous observations. Finally, this allows us to give an explicit algorithm for the construction of the entire compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$. As an application of our result, we are also able to construct the ordinary commuting graph of the ring $\mathcal{M}_3(GF(p))$ from the compressed commuting graph, by blowing-up the vertices into cliques and removing the center of the ring and all the loops. The construction of $\Gamma(\mathcal{M}_3(GF(p)))$ was an open problem for several years, so this can also be considered as a significant result of the research.

Finally, we give here an outline of the thesis. In Chapter 2 we present some basic results from group theory and matrix theory that we need throughout the thesis. In Chapter 3 we introduce the compressed commuting graph of a unital ring and discuss its properties. In particular, we prove that our compression is the best possible for the categorical approach, since the underlying relation of equivalence is the coarsest one that still induces a functor. Furthermore, we characterize all infinite unital rings that have a finite compressed commuting graph.

The problem of construction of $\Lambda^1(\mathcal{M}_2(GF(p))$ is discussed in Chapter 4. It is detected that the problem has to be broken into several cases, depending on the Jordan canonical form of the matrix in question. In every case of the problem, we describe the subset of the set of vertices belonging to certain case. Combining the results from all the cases, we obtain a description of the set of all vertices of $\Lambda^1(\mathcal{M}_2(GF(p))$. We continue with the discussion on the set of edges, and prove the interesting fact that there are no edges between vertices represented by non-derogatory matrices other than loops, see Proposition 4.4. Applying this proposition we are able to describe the set of edges of $\Lambda^1(\mathcal{M}_2(GF(p))$. It turns out that the proposition mentioned above is of great importance also in the case of the ring of matrices of order 3 and may be useful even for matrices of higher order.

The description of the graph $\Lambda^1(\mathcal{M}_3(GF(p)))$ is given in Chapters 5 – 8. We start with the description of the set of vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$ in Chapter 5, using the same idea of breaking into cases as in Chapter 4. For each case separately, we determine the number of vertices corresponding to a given case and collect the results in a table that describes the set of all vertices. Next, we investigate the neighborhood of vertices in Chapter 6, going case by case. As a result we obtain the table containing the number of vertices from each case in the neighborhood of a vertex of a given type.

In Chapter 7 we use data obtained in Chapters 5 and 6 and construct the subgraph of $\Lambda^1(\mathcal{M}_3(GF(p)))$, induced on the union of the set of vertices from two cases, namely (B) and (E). An interesting connection between this subgraph and a projective plane is discovered, and this connection is crucial for the subgraph description. The description of the whole graph $\Lambda^1(\mathcal{M}_3(GF(p)))$ is finalized in Chapter 8. The goal is achieved by investigating how other types of vertices are attached to the subgraph induced on $V_{(B)} \cup V_{(E)}$. Furthermore, we also give an algorithm for the construction of the graph $\Lambda^1(\mathcal{M}_3(GF(p)))$.

In the last chapter, Chapter 9, we apply our results to the study of the usual commuting graph $\Gamma(\mathcal{M}_3(GF(p)))$. In particular, we give an algorithm for the construction of the graph $\Gamma(\mathcal{M}_3(GF(p)))$ from the graph $\Lambda^1(\mathcal{M}_3(GF(p)))$ and table from Chapter 5.

Chapter 2

Preliminaries

Since the main problem addressed in the thesis is the description of the compressed commuting graph of the ring of matrices $\mathcal{M}_3(GF(p))$, we first list some basic definitions and theorems from linear algebra that we will need in the thesis. Although most of the claims hold for matrices of arbitrary order we will formulate some of them only for matrices of order 3.

Theorem 2.1. *The characteristic polynomial of a matrix $A \in \mathcal{M}_3(GF(p))$ has the form*

$$p_A(\lambda) = -\lambda^3 + \operatorname{tr}(A)\lambda^2 - (A_{11} + A_{22} + A_{33})\lambda + \det(A),$$

where $\operatorname{tr}(A)$ is the trace of A, $A_{ii}, i = 1, 2, 3,$ are the co-factors of A and $\det(A)$ is the determinant of A.

Proof. Let $A \in \mathcal{M}_3(GF(p))$ be an arbitrary matrix. Then we have

$$\begin{aligned}
p_A(\lambda) &= \det(A - \lambda I)\\
&= \begin{vmatrix} a_{11}-\lambda & a_{12} & a_{13}\\ a_{21} & a_{22}-\lambda & a_{23}\\ a_{31} & a_{32} & a_{33}-\lambda \end{vmatrix}\\
&= (a_{11}-\lambda)(a_{22}-\lambda)(a_{33}-\lambda) + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}\\
&\quad - a_{31}(a_{22}-\lambda)a_{13} - a_{32}a_{23}(a_{11}-\lambda) - a_{21}a_{12}(a_{33}-\lambda)\\
&= (a_{11}a_{22} - a_{11}\lambda - a_{22}\lambda + \lambda^2)(a_{33}-\lambda) + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}\\
&\quad - a_{31}a_{22}a_{13} + a_{31}a_{13}\lambda - a_{32}a_{23}a_{11} + a_{32}a_{23}\lambda - a_{21}a_{12}a_{33} + a_{21}a_{12}\lambda\\
&= a_{11}a_{22}a_{33} - a_{11}a_{33}\lambda - a_{22}a_{33}\lambda + a_{33}\lambda^2\\
&\quad - a_{11}a_{22}\lambda + a_{11}\lambda^2 + a_{22}\lambda^2 - \lambda^3 + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}\\
&\quad - a_{31}a_{22}a_{13} + a_{31}a_{13}\lambda - a_{32}a_{23}a_{11} + a_{32}a_{23}\lambda - a_{21}a_{12}a_{33} + a_{21}a_{12}\lambda\\
&= -\lambda^3 + \lambda^2(a_{11} + a_{22} + a_{33}) - \lambda(a_{11}a_{33} + a_{22}a_{33} + a_{11}a_{12} - a_{31}a_{13} - a_{32}a_{23} - a_{21}a_{12})\\
&\quad + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{21}a_{12}a_{33}\\
&= -\lambda^3 + \operatorname{tr}(A)\lambda^2 - (A_{11} + A_{22} + A_{33})\lambda + \det(A).
\end{aligned}$$

This completes the proof. □

Definition 2.2. We say that a non-zero polynomial $q \in GF(p)[x]$ is an *annihilating* polynomial of matrix A if $q(A) = 0$.

Note that polynomial $q \in GF(p)[x]$ can be represented by a polynomial $\widehat{q} \in \mathbb{Z}[x]$. Evaluating this polynomial in the matrix A over the field $GF(p)$ we have $\widehat{q}(A) = q(A)$. So, from the point of evaluation of polynomials we can consider polynomials to be from $\mathbb{Z}[x]$.

The following theorem is known as the Cayley Hamilton theorem.

Theorem 2.3. *Every matrix $A \in \mathcal{M}_3(GF(p))$ is annihilated by its own characteristic polynomial, i.e.,*

$$p_A(A) = -A^3 + \operatorname{tr}(A) \cdot A^2 + (A_{11} + A_{22} + A_{33}) \cdot A + \det(A) \cdot I = 0$$

Proof. Let $A \in \mathcal{M}_3(GF(p))$ be an arbitrary matrix. Then we have

$$\begin{aligned} A - \lambda I &= \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} - \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} \\ &= \begin{bmatrix} a_{11} - \lambda & a_{12} & a_{13} \\ a_{21} & a_{22} - \lambda & a_{23} \\ a_{31} & a_{32} & a_{33} - \lambda \end{bmatrix}. \end{aligned}$$

The adjoint matrix of $A - \lambda I$ is equal to

$$\operatorname{Adj}(A - \lambda I) = \begin{bmatrix} (A - \lambda I)_{11} & (A - \lambda I)_{21} & (A - \lambda I)_{31} \\ (A - \lambda I)_{12} & (A - \lambda I)_{22} & (A - \lambda I)_{32} \\ (A - \lambda I)_{13} & (A - \lambda I)_{23} & (A - \lambda I)_{33} \end{bmatrix},$$

where all of the entries are polynomials in λ with maximal degree 2. For example

$$\begin{aligned} (A - \lambda I)_{12} &= (-1)^{1+2} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} - \lambda \end{vmatrix} \\ &= -(a_{21}(a_{33} - \lambda) - a_{31}a_{23}) \\ &= -(a_{21}a_{33} - a_{21}\lambda - a_{31}a_{23}) \\ &= -a_{21}a_{33} + a_{21}\lambda + a_{31}a_{23}) \\ &= a_{21}\lambda + (a_{31}a_{23} - a_{21}a_{33}), \end{aligned}$$

whose degree is 1, or

$$\begin{aligned} (A - \lambda I)_{11} &= (-1)^{1+1} \begin{vmatrix} a_{22} - \lambda & a_{23} \\ a_{32} & a_{33} - \lambda \end{vmatrix} \\ &= (a_{22} - \lambda)(a_{33} - \lambda) - a_{32}a_{23} \\ &= \lambda^2 - (a_{22} + a_{33})\lambda + a_{22}a_{33} - a_{23}a_{32}, \end{aligned}$$

of degree 2. So, all the entries in matrix $\mathrm{Adj}(A-\lambda I)$ are polynomials with maximal degree 2, i.e., $\mathrm{Adj}(A-\lambda I) \in \mathcal{M}_3(GF(p)[\lambda])$. We can collect the coefficients of quadratic terms from all entries and form a matrix B_2, collect the coefficients of linear terms from all entries and form a matrix B_1 and collect the coefficients of free terms from all entries and form a matrix B_0. Now, matrix $\mathrm{Adj}(A-\lambda I)$ can be written as

$$\mathrm{Adj}(A-\lambda I) = B_2\lambda^2 + B_1\lambda + B_0, \tag{2.1}$$

in other words, $\mathrm{Adj}(A-\lambda I) \in \Big(\mathcal{M}_3\big(GF(p)\big)\Big)[\lambda]$.

From [27, Chapter VII, Proposition 3.7] we know that

$$\mathrm{Adj}(M)\cdot M = M \cdot \mathrm{Adj}(M) = \det(M)\cdot I.$$

Taking $M = A-\lambda I$, we have

$$(A-\lambda I)\,\mathrm{Adj}(A-\lambda I) = \det(A-\lambda I)I, \tag{2.2}$$

where we recognize the characteristic polynomial on the right side of equation (2.2), i.e.,

$$(A-\lambda I)\,\mathrm{Adj}(A-\lambda I) = p_A(\lambda)I.$$

If we use equation (2.1) on the left side of (2.2) and Theorem 2.1 on the right side, we get

$$\begin{gathered}
(A-\lambda I)(B_2\lambda^2 + B_1\lambda + B_0) = p_A(\lambda)I,\\
AB_2\lambda^2 + AB_1\lambda + AB_0 - B_2\lambda^3 - B_1\lambda^2 - B_0\lambda = \big(-\lambda^3 + tr(A)\lambda^2 - (A_{11}+A_{22}+A_{33})\lambda + \det(A)\big)I,\\
-B_2\lambda^3 + (AB_2 - B_1)\lambda^2 + (AB_1 - B_0)\lambda + AB_0 = -\lambda^3 I + tr(A)\lambda^2 I - (A_{11}+A_{22}+A_{33})\lambda I + \det(A)I.
\end{gathered}$$

Considered as an equality in $\Big(\mathcal{M}_3\big(GF(p)\big)\Big)[\lambda]$, the space of polynomials with matrix coefficients from $\mathcal{M}_3(GF(p))$, the last equality is equivalent to the system of four equalities in $\mathcal{M}_3\big(GF(p)\big)$, namely

$$\begin{cases}
-B_2 = -I,\\
AB_2 - B_1 = tr(A)I,\\
AB_1 - B_0 = -(A_{11}+A_{22}+A_{33})I,\\
AB_0 = \det(A)I.
\end{cases}$$

Multiplying the first equation with A^3 from the left, the second with A^2 and third with A, we get

$$\begin{cases}
-A^3B_2 = -A^3,\\
A^3B_2 - A^2B_1 = tr(A)A^2,\\
A^2B_1 - AB_0 = -(A_{11}+A_{22}+A_{33})A,\\
AB_0 = \det(A)I.
\end{cases}$$

Adding all the right sides, we obtain

$$-A^3 + tr(A)A^2 - (A_{11} + A_{22} + A_{33})A + \det(A)I$$

which is obviously $p_A(A)$. Adding all the left sides, we get 0, hence

$$p_A(A) = 0,$$

which is what we wanted to prove. □

One of the annihilating polynomials is of particular interest for our topic.

Definition 2.4. Polynomial $m_A \in GF(p)[x]$ is a *minimal* polynomial of matrix A if it satisfies the following conditions:

1) $m_A(A) = 0$,

2) m_A is monic, i.e., the leading coefficient of m_A is 1, and

3) if $q \in GF(p)[x]$ is any non-zero polynomial that annihilates matrix A, then $\deg(m_A) \leq \deg(q)$.

In next proposition we prove a basic property of minimal polynomial.

Proposition 2.5. *For every matrix $A \in \mathcal{M}_3(GF(p))$ there exists a unique minimal polynomial m_A.*

Proof. First, the set of annihilating polynomials has at least one monic member, because $-p_A$ is a monic annihilating polynomial by Theorem 2.3. So, there exists an annihilating polynomial of the smallest degree. If we normalize this polynomial to be monic, we get a minimal polynomial. Therefore, A has at least one minimal polynomial m_A. To prove uniqueness, suppose that m_A^1 and m_A^2 are two different minimal polynomials of A. Then $m_A^1 - m_A^2$ is non-zero by assumption, and is an annihilating polynomial of A. But m_A^1 and m_A^2 have the same degree, and each has leading coefficient 1, so $m_A^1 - m_A^2$ has degree less than that of m_A. This contradicts the minimality of the degree of m_A. □

The following proposition connects minimal and annihilating polynomials.

Proposition 2.6. *For any polynomial s we have $s(A) = 0$ if and only if m_A divides s.*

Proof. If m_A divides s then clearly $s(A) = 0$. To prove the converse, we use the result known as Euclid's algorithm or "the division algorithm" which implies that for polynomials s and m_A there are polynomials q and r such that $s = q \cdot m_A + r$ and r is either the zero polynomial or has degree less than that of m_A. Now, $r(A) = s(A) - q(A) \cdot m_A(A) = 0 - 0 = 0$, so by definition of minimal polynomial $r = 0$. Hence m_A divides s. □

In next theorem we consider the eigenvalues of a matrix $A \in \mathcal{M}_3(GF(p))$ as elements of the algebraic closure of $GF(p)$.

Theorem 2.7. *Any eigenvalue of a matrix $A \in \mathcal{M}_3(GF(p))$ is a root of its minimal polynomial, so the minimal polynomial and the characteristic polynomial have the same roots.*

Proof. Say λ is an eigenvalue of a matrix A in the algebraic closure $\overline{GF(p)}$. We want to show that $m_A(\lambda) = 0$. There is an eigenvector $v \neq 0$ in $\overline{GF(p)}^3$ for this eigenvalue, i.e., $Av = \lambda v$. Then $A^k v = \lambda^k v$, for all $k \geq 1$, so $f(A)v = f(\lambda)v$ for all $f \in GF(p)[x]$. In particular, taking $f(x) = m_A(x)$, we have $m_A(A) = 0$ so $0 = m_A(\lambda)v$. Thus $m_A(\lambda) = 0$. □

Theorem 2.8. *Irreducible factors of the characteristic polynomial of A are factors of the minimal polynomial of A and vice versa.*

Proof. Any irreducible factor of the minimal polynomial of A is a factor of the characteristic polynomial since the minimal polynomial divides the characteristic polynomial, as a consequence of Cayley Hamilton theorem and Proposition 2.6. Conversely, if $\pi(x)$ is an irreducible factor of the characteristic polynomial, a root of it, possibly in the extension field, is an eigenvalue and therefore is also a root of the minimal polynomial by Theorem 2.7. Any polynomial in $GF(p)[x]$ sharing a root with $\pi(x)$ is divisible by $\pi(x)$, so $\pi(x)$ divides the minimal polynomial. □

Theorem 2.9. *Suppose $A \in \mathcal{M}_3(GF(p))$ is a block-diagonal matrix with A_1 and A_2 as the diagonal blocks, i.e.,*

$$A = \begin{bmatrix} A_1 & \\ & A_2 \end{bmatrix}.$$

Then the minimal polynomial of A is the least common multiple (lcm) *of the minimal polynomials of A_1 and A_2.*

Proof. Let $m_A(x)$ be the minimal polynomial of A, $m_{A_1}(x)$ and $m_{A_2}(x)$ the minimal polynomials of A_1 and A_2, respectively. According to Definition 2.4 we have $m_A(A) = 0$ which is equivalent to

$$m_A(A) = m_A\Big(\begin{bmatrix} A_1 & \\ & A_2 \end{bmatrix} \Big) = \begin{bmatrix} m_A(A_1) & \\ & m_A(A_2) \end{bmatrix} = \begin{bmatrix} 0 & \\ & 0 \end{bmatrix}.$$

Last equality implies $m_A(A_1) = 0$ and $m_A(A_2) = 0$. Now, from Proposition 2.6 we have m_{A_1} divides m_A and m_{A_2} divides m_A, so

$$\text{lcm}(m_{A_1}, m_{A_2}) \text{ divides } m_A. \tag{2.3}$$

Let f be an arbitrary polynomial such that m_{A_1} divides f and m_{A_2} divides f. Then we have

$$f(A) = \begin{bmatrix} f(A_1) & \\ & f(A_2) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

so $f(A) = 0$. By Proposition 2.6 we conclude $m_A(x)$ divides f. Therefore, if we take $f = \operatorname{lcm}(m_{A_1}, m_{A_2})$ we obtain

$$m_A(x) \text{ divides } \operatorname{lcm}(m_{A_1}, m_{A_2}). \tag{2.4}$$

From (2.3) and (2.4) we get $m_A(x) = \operatorname{lcm}(m_{A_1}, m_{A_2})$. □

Let us recall one of the basic concepts when we talk about commutativity.

Definition 2.10. The *centralizer* of a matrix A from $\mathcal{M}_n(GF(p))$, denoted by $\mathscr{C}(A)$, is the set of all matrices from $\mathcal{M}_n(GF(p))$ which commute with A, i.e.,

$$\mathscr{C}(A) = \{X \in \mathcal{M}_n(GF(p)) : AX = XA\}.$$

Note that the intersection of the centralizers of all matrices is the *center* of the ring of matrices $\mathcal{M}_3(GF(p))$ and is denoted by $Z(\mathcal{M}_3(GF(p)))$.

Definition 2.11. A *non-derogatory* matrix is one, whose minimal polynomial equals its characteristic polynomial, up to a sign, while a matrix is *derogatory*, if they do not coincide.

The following characterization of the non-derogatory matrices is taken from [18].

Theorem 2.12. *For a matrix $A \in \mathcal{M}_n(GF(p))$ the following statements are equivalent:*

(*i*) *A is non-derogatory,*

(*ii*) $\mathscr{C}(A) = \langle A \rangle_1$.

Proof. From [18, Theorem 2.8] it follows that for integer $n \geq 2$ and a field $\mathbb{F}$ such that $|\mathbb{F}| \geq n$ a matrix A from $\mathcal{M}_n(\mathbb{F})$ is non-derogatory if and only if $\mathscr{C}(A) = \mathbb{F}[A]$, where $\mathbb{F}[A]$ denotes the unital subalgebra generated by A.

We claim that the above is true even without the restrictions on n and $|\mathbb{F}|$. Suppose n and $\mathbb{F}$ are arbitrary. First, note that if $n = 1$ then every matrix A is non-derogatory and satisfies the equality $\mathscr{C}(A) = \mathbb{F}[A]$. Assume $n \geq 2$ and denote by $\overline{\mathbb{F}}$ the algebraic closure of the field $\mathbb{F}$. Now, let $A \in \mathcal{M}_n(\mathbb{F})$. Denote the minimal polynomial of A over $\mathbb{F}$ by m_A, and denote the minimal polynomial of A over $\overline{\mathbb{F}}$ by $\overline{m_A}$. We claim that

$$m_A = \overline{m_A}. \tag{2.5}$$

Suppose $\overline{m_A}(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ where a_i are from $\overline{\mathbb{F}}$. Then $a_0, a_1, \ldots, a_{k-1}$ are solution of matrix equation $\overline{m_A}(A) = 0$, where the coefficients of $\overline{m_A}$ are viewed as variables. This equation is equivalent to a system of n^2 linear equations with coefficient in $\mathbb{F}$. Since this system has a solution in $\overline{\mathbb{F}}$, the Gaussian algorithm implies that it has a solution also in $\mathbb{F}$. This implies that $\deg m_A \leq \deg \overline{m_A}$. Since m_A is annihilating polynomial of A and $\overline{m_A}$ is the minimal polynomial with coefficient in $\overline{\mathbb{F}}$ it holds that $\overline{m_A}$ divides m_A. Combining the two conditions we get $\overline{m_A} = m_A$.

Denote by $\mathscr{C}(A)$ the centralizer of A inside $\mathcal{M}_n(\mathbb{F})$ and by $\overline{\mathscr{C}}(A)$ the centralizer of A inside $\mathcal{M}_n(\overline{\mathbb{F}})$. We claim that

$$\dim_{\mathbb{F}} \mathscr{C}(A) = \dim_{\overline{\mathbb{F}}} \overline{\mathscr{C}}(A). \tag{2.6}$$

The set $\overline{\mathscr{C}}(A)$ is the set of solutions from $\mathcal{M}_n(\overline{\mathbb{F}})$ of the matrix equation $XA = AX$. This equation is equivalent to the system of n^2 linear equations with coefficients in $\mathbb{F}$. Denote the matrix of the system by M. Then, M is the element of $\mathcal{M}_{n^2}(\mathbb{F})$. Furthermore, $\dim_{\overline{\mathbb{F}}} \overline{\mathscr{C}}(A)$ is equal to the rank of matrix M. The same conclusions hold for $\mathscr{C}(A)$, because M is not changed. This proves equation (2.6).

Equation (2.5) implies that $A \in \mathcal{M}_n(\mathbb{F})$ is non-derogatory if and only if $A \in \mathcal{M}_n(\overline{\mathbb{F}})$ is non-derogatory. Furthermore, equations (2.5) and (2.6) imply that the condition $\mathscr{C}(A) = \mathbb{F}[A]$ is equivalent to $\overline{\mathscr{C}}(A) = \overline{\mathbb{F}}[A]$. The condition $\mathscr{C}(A) = \mathbb{F}[A]$ is equivalent to $\dim_{\mathbb{F}} \mathscr{C}(A) = \deg m_A$. By equations (2.5) and (2.6) the later condition is equivalent to $\dim_{\overline{\mathbb{F}}} \overline{\mathscr{C}}(A) = \deg \overline{m_A}$. This is further equivalent to $\overline{\mathscr{C}}(A) = \overline{\mathbb{F}}[A]$.

Since $\overline{\mathbb{F}}$ is not finite, it holds $|\overline{\mathbb{F}}| > n$, so from [18, Theorem 2.8] that the conditions

(a) $A \in \mathcal{M}_n(\overline{\mathbb{F}})$ is non-derogatory,

(b) $\overline{\mathscr{C}}(A) = \overline{\mathbb{F}}[A]$,

are equivalent, hence, by the above, the conditions

(c) $A \in \mathcal{M}_n(\mathbb{F})$ is non-derogatory,

(d) $\mathscr{C}(A) = \mathbb{F}[A]$,

are also equivalent. In our case $\mathbb{F} = GF(p)$, so that $\mathbb{F}[A] = \langle A \rangle_1$, and the claim follows. □

Definition 2.13. The *kernel* of a matrix $A \in \mathcal{M}_3(GF(p))$, also called the null space of a matrix A, is the kernel of the linear map $\mathcal{A} : GF(p)^3 \to GF(p)^3$ defined by A, i.e.,

$$\operatorname{Ker} A = \{v \in GF(p)^3 : \mathcal{A}(v) = 0\} = \{v \in GF(p)^3 : A \cdot v = 0\}.$$

Definition 2.14. The *image* of a matrix $A \in \mathcal{M}_3(GF(p))$, is the image of the linear map $\mathcal{A} : GF(p)^3 \to GF(p)^3$ defined by $v \mapsto Av$, i.e.,

$$\operatorname{Im} A = \{\mathcal{A}(v) : v \in GF(p)^3\} = \{Av : v \in GF(p)^3\}.$$

In what follows we will introduce the Jordan form of a given matrix. We remark that Jordan form of a matrix is usually defined over the algebraic closure of the base field, but here we will need the Jordan form over the base field, when it exists.

Definition 2.15. A Jordan block $J_{\lambda,k}$ is a square matrix over the field $GF(p)$ of the form

$$J_{\lambda,k} = \begin{bmatrix} \lambda & 1 & & & & \\ & \lambda & 1 & & & \\ & & \ddots & \ddots & & \\ & & & \lambda & 1 & \\ & & & & \lambda & 1 \\ & & & & & \lambda \end{bmatrix}_{k\times k} \tag{2.7}$$

where the missing entries are all zero.

Definition 2.16. A square matrix J over the field $GF(p)$ is said to be in *Jordan form* if it is block diagonal where each diagonal block is a Jordan block.

$$J = \begin{bmatrix} J_{\lambda_1,k_1} & & & \\ & J_{\lambda_2,k_2} & & \\ & & \ddots & \\ & & & J_{\lambda_l,k_l} \end{bmatrix}_{n\times n} \tag{2.8}$$

where $n = k_1 + k_2 + \cdots + k_l$ and the missing entries are all zero.

We omit the proofs of the following propositions for the sake of brevity. They can be found in [31].

Proposition 2.17. *Let A be a square matrix over the field $GF(p)$. If the minimal polynomial of A splits into linear factors over $GF(p)$ then there exists a square matrix J in Jordan form, similar to matrix A. It is said that A has Jordan canonical form J.*

Proposition 2.18. *Jordan canonical form of a square matrix A is unique up to the order of Jordan blocks.*

Proposition 2.19. *Let A be a square matrix over the field $GF(p)$ and $\lambda \in GF(p)$ be an eigenvalue of A. The geometric multiplicity of λ, i.e., the dimension of the $\lambda-$eigenspace of A, is equal to the number of Jordan blocks in the Jordan form of the matrix A.*

Proposition 2.20. *The size of the largest Jordan block corresponding to an eigenvalue $\lambda \in GF(p)$ of A is exactly the degree of the term $(x-\lambda)$ in the minimal polynomial of A, i.e., the algebraic multiplicity of eigenvalue λ.*

Next, we calculate the number of invertible matrices of order n.

Proposition 2.21. *The number of invertible matrices in $\mathcal{M}_n(GF(p))$ is equal to*

$$|GL_n(GF(p))| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

Proof. In order for an $n \times n$ matrix to be invertible, we need the rows to be linearly independent. Clearly, we have $p^n - 1$ choices for the first row. Now, there are p vectors in the span of the first row, so we have $p^n - p$ choices for the second row. Now, let v_1, v_2 be the first two rows. Then the set of vectors in the span of v_1, v_2 is of the form $\{c_1 v_1 + c_2 v_2 : c_1, c_2 \in GF(p)\}$. This set is of size p^2, as we have p choices for c_1 and p choices for c_2. Thus, we have $p^n - p^2$ choices for the third row. Continuing this way gives the desired formula. □

Later on, we will need the center of the ring of matrices, so we determine it in next proposition.

Proposition 2.22. *The center of $\mathcal{M}_n(GF(p))$ consists of the scalar multiples of the identity matrix, i.e.,*

$$Z(\mathcal{M}_n(GF(p)) = GF(p)I.$$

Proof. Suppose $A \in \mathcal{M}_n(GF(p))$. Let $E_{i,j}$ be the matrix whose (i,j) entry is $1 \in GF(p)$, and all other entries are $0 \in GF(p)$. Then the equations

$$E_{i,i} \cdot A = A \cdot E_{i,i}, \quad i = 1, 2, 3,$$

imply that A is necessarily diagonal. Furthermore, equations

$$E_{i,j} \cdot A = A \cdot E_{i,j}, \quad 1 \leq i \neq j \leq n,$$

imply that $a_{i,i} = a_{j,j}$ for all $i, j \in \{1, 2, \ldots, n\}$. Consequently, there exists $a \in GF(p)$ such that $A = aI$. □

Recall that the group of invertible matrices $GL_n(GF(p))$ acts on the set of all matrices $\mathcal{M}_n(GF(p))$ by conjugation. The orbit of a given matrix A with respect to this action is

$$\mathcal{O}(A) = \{M \in \mathcal{M}_n(GF(p)) : M \,\text{similar to}\, A\}.$$

In next proposition we calculate the cardinality of the orbit.

Proposition 2.23. *Let $A \in \mathcal{M}_n(GF(p))$. Then*

$$|\mathcal{O}(A)| = \frac{\big|GL_n(GF(p))\big|}{\big|\mathscr{C}(A) \cap GL_n(GF(p))\big|}.$$

Proof. Note that

$$|\mathcal{O}(A)| = |\{M \in \mathcal{M}_n(GF(p)) : M \,\text{similar to}\, A\}| = |\{SAS^{-1} : S \in GL_n(GF(p))\}|.$$

Two invertible matrices $S, T \in GL_n(GF(p))$ induce the same matrix $SAS^{-1} = TAT^{-1}$ if and only if $T^{-1}SA = AT^{-1}S$, which is equivalent to $T^{-1}S \in \mathscr{C}(A)$. This is further equivalent to $S\boldsymbol{H} = T\boldsymbol{H}$ where $\boldsymbol{H} = \mathscr{C}(A) \cap GL_n(GF(p))$ is a subgroup of $GL_n(GF(p))$. Hence,

$$|\mathcal{O}(A)| = |GL_n(GF(p))/\boldsymbol{H}| = \frac{|GL_n(GF(p)|}{|\mathscr{C}(A) \cap GL_n(GF(p))|}.$$

□

Next proposition gives some of the similarity invariants that will be used in our arguments.

Proposition 2.24. *Suppose A and B are matrices over the field $\mathbb{F}$. If A and B are similar matrices then*

1) $\dim \operatorname{Ker} A = \dim \operatorname{Ker} B$,

2) A and B have the same eigenvalues with the same algebraic and geometric multiplicities.

Proof. 1) As B is similar to A there exists an invertible matrix S such that $B = SAS^{-1}$. Last equation is equivalent to $S^{-1}B = AS^{-1}$. Observe that if $x \in \operatorname{Ker} B$ then $S^{-1}x \in \operatorname{Ker} A$.

We claim that if $\{v_1, v_2, \dots v_k\}$ is a basis for $\operatorname{Ker} B$ then the vectors $S^{-1}v_1, S^{-1}v_2, \dots, S^{-1}v_k$ are linearly independent. Suppose $c_i \in GF(p)$ for each $i = 1, 2, \dots, k$ are such that

$$c_1S^{-1}v_1 + c_2S^{-1}v_2 + \cdots + c_kS^{-1}v_k = 0.$$

By linearity we can move the constants in-between the matrix and the vectors and then by the linearity again we can pull S^{-1} out so we get

$$S^{-1}(c_1v_1 + c_2v_2 + \cdots c_kv_k) = 0.$$

However, S^{-1} is invertible so if we multiply by S we get

$$c_1v_1 + c_2v_2 + \cdots c_kv_k = 0.$$

Since $v_1, v_2, \dots v_k$ are linearly independent, we have $c_1 = c_2 = \cdots = c_k = 0$, so the vectors $S^{-1}v_1, S^{-1}v_2, \dots, S^{-1}v_k$ are linearly independent. Furthermore, vectors $S^{-1}v_1, S^{-1}v_2, \dots, S^{-1}v_k$ belong to $\operatorname{Ker} A$, which implies that

$$\dim \operatorname{Ker} B \leq \dim \operatorname{Ker} A. \tag{2.9}$$

Similarly, by reversing the roles of A and B we get the other inequality

$$\dim \operatorname{Ker} A \leq \dim \operatorname{Ker} B. \tag{2.10}$$

Conjunction of inequalities (2.9) and (2.10) is equivalent to equality *1)*.

2) Note that $p_B(x) = \det(B - \lambda I) = \det(SAS^{-1} - S\lambda IS^{-1}) = \det(S(A - \lambda I)S^{-1}) = \det(A - \lambda I) = p_A(x)$. This proves that every common eigenvalue of A and B has the same algebraic multiplicity. Using statement *1)* it is obvious that corresponding geometric multiplicities are equal. □

Chapter 3

Compressed commuting graph of a unital ring

We will assume throughout this chapter that R is a unital ring with identity element 1. In what follows, we will introduce the commuting graph $\Gamma(R)$ as defined in [2] and the compressed commuting graph of unital ring $\Lambda^1(R)$ as defined in [13].

Definition 3.1. A *commuting graph* of a unital ring R is an undirected graph $\Gamma(R)$ whose vertex set is the set of all non-central elements of R and there is an edge between two different elements a and b if and only if $ab = ba$.

Definition 3.2. A unital subring of R generated by an element a from R will be denoted by $\langle a \rangle_1$, i.e.,

$$\langle a \rangle_1 = \{q(a) \mid q \in \mathbb{Z}[x]\}, \tag{3.1}$$

where $\mathbb{Z}[x]$ denotes the ring of polynomials with integer coefficients and in the evaluation of $q(a)$ the constant term is multiplied by the identity element 1.

We introduce an equivalence relation $\sim$ on R defined by $a \sim b$ if and only if $\langle a \rangle_1 = \langle b \rangle_1$, and denote the equivalence class of an element $a \in R$ with respect to relation $\sim$ by $[a]_1$. By definition $[a]_1$ consists of all single generators of the ring $\langle a \rangle_1$.

Definition 3.3. A *unital compressed commuting graph* of a unital ring R is an undirected graph $\Lambda^1(R)$ whose vertex set is the set of all equivalence classes of elements of R with respect to relation $\sim$ and there is an edge between $[a]_1$ and $[b]_1$ if and only if $ab = ba$.

We need to prove that edges in $\Lambda^1(R)$ are well defined. Suppose that $[a]_1 = [a']_1$, $[b]_1 = [b']_1$, and $ab = ba$, then $a' \in \langle a \rangle_1$ and $b' \in \langle b \rangle_1$, hence, $a', b' \in \langle a, b \rangle_1$, the subring generated by two elements a and b. But since a and b commute, $\langle a, b \rangle_1$ is a commutative ring, hence a' and b' commute as well. It should be remarked that central elements of R are not excluded from the graph $\Lambda^1(R)$ like in the usual commuting graph $\Gamma(R)$. Furthermore, loops are allowed in $\Lambda^1(R)$, in fact, every vertex of $\Lambda^1(R)$ has a single loop on it.

In [13] the authors also introduce a non-unital version of the compressed commuting graph, denoted by $\Lambda(R)$, however, here we will be interested in unital version only, hence, we will often omit the adjective "unital" and simply speak about compressed commuting graph. The reader can find the connection between the two versions of the graph in the [13].

Note an important fact that each vertex of $\Lambda^1(R)$ corresponds to a subring of R generated by one element. This means that we could equivalently define the compressed commuting graph of R as an undirected graph whose vertex set is the set

$$V(\Lambda^1(R)) = \{\langle a\rangle_1 \mid a \in R\},$$

the set of all subrings of R generated by one element, and vertices $\langle a\rangle_1$ and $\langle b\rangle_1$ are connected by an edge if and only if $ab = ba$.

The mapping Λ^1 can be extended to a functor Λ^1 from the category $\mathbf{Ring^1}$ of unital rings and unital ring homomorphisms to the category **Graph** of undirected simple graphs that allow loops and graph homomorphisms. For a ring homomorphism $f\colon R \to S$, where R and S are unital rings, we define a graph homomorphism $\Lambda^1(f)\colon \Lambda^1(R) \to \Lambda^1(S)$ by $\Lambda^1(f)([r]_1) = [f(r)]_1$. We need to verify that the map $\Lambda^1(f)$ is well defined. If $[r]_1 = [r']_1$ then there exist polynomials $p, q \in \mathbb{Z}[x]$ such that $r' = p(r)$ and $r = q(r')$. Hence, $f(r') = p(f(r))$ and $f(r) = q(f(r'))$ and consequently $[f(r)]_1 = [f(r')]_1$. Furthermore, $\Lambda^1(f)$ maps connected vertices to connected vertices since $ab = ba$ implies $f(a)f(b) = f(b)f(a)$. So the map $\Lambda^1(f)$ is indeed a graph homomorphism. Here the zero ring $R = 0$ is considered as a unital ring with $1 = 0$. It is easy to check that $\Lambda^1(\mathrm{id}_R) = \mathrm{id}_{\Lambda^1(R)}$ for any ring R and $\Lambda^1(f \circ g) = \Lambda^1(f) \circ \Lambda^1(g)$ for all unital ring homomorphisms $f\colon S \to T$ and $g\colon R \to S$. This proves the following.

Proposition 3.4. *The mapping $\Lambda^1\colon \mathbf{Ring}^1 \to \mathbf{Graph}$ that maps a unital ring R to the graph $\Lambda^1(R)$ and a ring homomorphism f to the graph homomorphism $\Lambda^1(f)$ is a functor.*

The following gives the motivation for choosing the particular equivalence relation in Definition 3.3. It implies that, at least on finite unital algebras, the relation $\sim$ is the coarsest relation that still induces a functor.

Theorem 3.5. *For each unital ring R let $\approx_R$ be an equivalence relation on R such that the family $\{\approx_R \mid R \text{ a unital ring}\}$ induces a well defined functor $F\colon \mathbf{Ring^1} \to \mathbf{Graph}$ in the following way:*

(i) For each unital ring R the vertices of $F(R)$ are equivalence classes $[r]_{\approx_R}$ of elements of R with respect to $\approx_R$ and there is an edge between $[a]_{\approx_R}$ and $[b]_{\approx_R}$ if and only if $ab = ba$.

(ii) For each unital ring homomorphism $f\colon R \to S$, where R and S are unital rings, the graph homomorphism $F(f)\colon F(R) \to F(S)$ is given by $F(f)([r]_{\approx_R}) = [f(r)]_{\approx_S}$ for all $r \in R$.

Then for any finite unital algebra A and for any $a, b \in A$ the condition $a \approx_A b$ implies $a \sim b$.

Proof. Let A be a finite unital algebra. Since it is finite, it is an algebra over a finite field $\mathbb{F}$, the characteristic of $\mathbb{F}$ is a prime p, and its prime field is $GF(p)$. Thus, we may consider A as a finite dimensional algebra over $GF(p)$. Hence, the algebra $E = \mathrm{End}_{GF(p)}(A)$ of all $GF(p)$-linear transformations on A is isomorphic to a matrix algebra $\mathcal{M}_n(GF(p))$, where $n = \dim_{GF(p)} A$. Let $L\colon A \to E$ be the left regular representation of A given by $L(a) = L_a$ for all $a \in A$, where L_a denotes left multiplication by a. Now suppose $a \approx_A b$ holds in A. Since L is a unital ring homomorphism, item (ii) implies that $L_a \approx_E L_b$. The fact that edges in item (ii) must be well defined implies $\mathscr{C}(L_a) = \mathscr{C}(L_b)$. Since E is isomorphic to a full matrix algebra, it follows from the Centralizer Theorem [30, p. 113, Corollary 2] that this is equivalent to $GF(p)[L_a] = GF(p)[L_b]$, where $GF(p)[L_a]$ denotes the unital $GF(p)$-algebra generated by L_a, see [18, Lemma 2.4]. But $GF(p) \cong \mathbb{Z}_p$ is a factor ring of $\mathbb{Z}$, so that $GF(p)[L_a] = \langle L_a \rangle_1$ and consequently $\langle L_a \rangle_1 = \langle L_b \rangle_1$. Hence, there exist polynomials $P, Q \in \mathbb{Z}[x]$ such that $L_a = P(L_b) = L_{P(b)}$ and $L_b = Q(L_a) = L_{Q(a)}$. Applying these transformations to $1 \in A$ gives $a = P(b)$ and $b = Q(a)$, hence $\langle a \rangle_1 = \langle b \rangle_1$ and $a \sim b$. □

Since the motivation for the compression is to make a graph smaller it is interesting to ask whether an infinite unital ring can have a finite compressed commuting graph. In the paper [14] it is shown that this is indeed possible and it is also possible to classify all such rings.

Theorem 3.6. *If R is an infinite unital ring, then either $|V(\Lambda^1(R))| = |R|$ or R is isomorphic to a unital semidirect product $\mathbb{Z}[\frac{1}{m}] \ltimes I$ for some positive integer m and some finite $\mathbb{Z}[\frac{1}{m}]$-ring I. In the later case we have $|R| = \aleph_0$ and $|V(\Lambda^1(R))| < \aleph_0$.*

We omit the proof of the theorem and the reader can find it in [14]. In this thesis our focus will be on finite rings of matrices over $GF(p)$ of orders 2 and 3. In next chapter we will start with matrices of order 2.

Chapter 4

Compressed commuting graph of $\mathcal{M}_2(GF(p))$

Since any similarity is a ring isomorphism, it induces a graph isomorphism, see Proposition 3.4. This means that similar matrices will behave the same way in the compressed commuting graph construction process. When considering a specific matrix we can consider its nicest possible form which will be the Jordan canonical form in the case when all the zeros of the characteristic polynomial lie in the field $GF(p)$ and if not we will use the companion matrix instead.

Therefore, the problem of describing the vertices of the compressed commuting graph of the ring $\mathcal{M}_2(GF(p))$ will be divided into the following cases depending on how the characteristic polynomial of a matrix splits over the field $GF(p)$.

Case (A): Diagonalizable matrices with one double eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}.$$

Case (B): Diagonalizable matrices with two different eigenvalues λ and μ from $GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

Case (C): Non-diagonalizable matrices with one double eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

Case (D): Matrices whose characteristic polynomial is irreducible over $GF(p)$, i.e., with no eigenvalues in the field $GF(p)$.

We will refer to matrices from case (X) as matrices of type (X).

Proposition 4.1. *Suppose A and B are two matrices from $\mathcal{M}_2(GF(p))$. If $\langle A\rangle_1 = \langle B\rangle_1$ then A and B are of the same type.*

Proof. First note that $\deg m_A = \deg m_B$. We consider two cases, depending on the degree of m_A. Assume first that $\deg m_A = 1$. In this case matrix A is clearly a scalar matrix. Then $\langle A\rangle_1 = GF(p)I$, so B is also scalar matrix and this means that both of them are of type (A). Now assume that $\deg m_A = 2$. Further, we will discuss two subcases, depending whether m_A splits over $GF(p)$ or not.

Assume first that m_A splits. It means that matrix A is similar to a matrix in Jordan form. Without lost of generality we can assume that A is in Jordan form. As $\langle A\rangle_1 = \langle B\rangle_1$ there exist polynomials q and r such that $B = q(A)$ and $A = r(B)$. This implies that the number of different eigenvalues is the same for both matrices. If the mentioned number is 2 then matrices are both diagonalizable so they are of type (B). On the other hand, if the number is 1 then matrix A and Jordan form of matrix B have only one Jordan block, i.e., they are of type (C).

Finally, assume that m_A does not split, so m_A is irreducible and A is of type (D). Eigenvalues of A are not in $GF(p)$ so as $A = r(B)$, eigenvalues of B are not in the $GF(p)$ either, i.e., $p_B = m_B$ is irreducible, which means that B is of type (D) as well. This completes the proof. □

From Proposition 4.1 we know that all matrices that will be compressed into one vertex are matrices of the same type. This means that we can speak about the type of a vertex in the compressed commuting graph.

Similarly as for the matrices from $\mathcal{M}_2(GF(p))$ the breaking into cases will also be done for matrices from $\mathcal{M}_3(GF(p))$ in Chapter 5. The following definition and proposition are valid for both $n = 2$ and $n = 3$.

Definition 4.2. Define $V_{(X)} \subseteq V(\Lambda^1(\mathcal{M}_n(GF(p)))$ as the set of vertices of type (X), where $n = 2$ or $n = 3$.

Proposition 4.3. *Suppose we have a vertex of type (X), represented by a matrix A of order n, where $n = 2$ or $n = 3$. Assume that $\mathcal{O}(A)$ intersects every vertex of type (X) and let*

$$\omega_A = |\langle A\rangle_1 \cap \mathcal{O}(A)|. \tag{4.1}$$

Then

$$|V_{(X)}| = \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_n(GF(p))|}{|\mathscr{C}(A) \cap GL_n(GF(p))| \cdot \omega_A}. \tag{4.2}$$

Proof. As shown in the proof of Proposition 2.23, some of the matrices similar to the matrix A lie inside the subring $\langle A\rangle_1$, but some of them do not. Those which do not will be generators of the isomorphic copies of the subring $\langle A\rangle_1$. To count the number of vertices of type (X), we will need to count how many matrices similar to A lie in the subring $\langle A\rangle_1$.

Let $M \in \mathcal{O}(A)$ be arbitrary. Then M is similar to A, i.e., there exists an invertible matrix S such that $M = SAS^{-1}$. The conjugation mapping $Y \mapsto SYS^{-1}$ is bijection from set $\langle A\rangle_1 \cap \mathcal{O}(A)$

to the set $\langle M\rangle_1 \cap \mathcal{O}(A)$, so all of the sets $\langle M\rangle_1 \cap \mathcal{O}(A)$, $M \in \mathcal{O}(A)$, are of the same cardinality and this cardinality is equal to ω_A.

Note that any W from $\langle M\rangle_1 \cap \mathcal{O}(A)$ is automatically a generator of $\langle M\rangle_1$. This is because W is similar to A and hence similar to M, so three of them have the same degree of minimal polynomial, see Proposition 2.24. Since W is from $\langle M\rangle_1$ this implies that W is a generator of $\langle M\rangle_1$. Hence, matrices in $\langle M\rangle_1 \cap \mathcal{O}(A)$ are compressed into the same vertex.

It follows that the number of vertices obtained from matrices of type (X) is equal to

$$|V_{(X)}| = \frac{|\mathcal{O}(A)|}{\omega_A}.$$

Equation (4.2) now follows from Proposition 2.23. □

Now, we consider the cases and calculate the number of vertices in $\Lambda^1(\mathcal{M}_2(GF(p)))$ of each type.

Case (A): Diagonalizable matrices with one double eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}.$$

Note that matrix A is a scalar matrix, i.e., $A = \lambda \cdot I$. For every matrix B similar to $A = \lambda I$ there exists invertible matrix S such that $B = SAS^{-1} = S\lambda IS^{-1} = \lambda I$ i.e., there are no matrices of type (A) except of p scalar matrices. No two of them are similar as they have different eigenvalues.

The minimal polynomial of A is $m_A(x) = x - \lambda$, which is of degree 1. This fact can be used to find general form of the element of the subring $\langle A\rangle_1$. Namely,

$$\begin{aligned} \langle A\rangle_1 &= \{q(A) : q \in \mathbb{Z}[x]\} = \{q(A) : q \in GF(p)[x]\} \\ &= \{q(A) : \deg(q) = 0\} = GF(p) \cdot I, \end{aligned}$$

This means that subring consists only of matrices of type (A), and subring contains every matrix from case (A).

As we discussed all of the previous calculations for arbitrary $A = \lambda I$, every matrix from the set $GF(p) \cdot I$ is generator of the unique subring $GF(p) \cdot I$. In other words, there are no proper subrings of the subring $\langle A\rangle_1$, i.e, all of the matrices from this case will be compressed into one point in $\Lambda^1(\mathcal{M}_2(GF(p)))$, i.e.,

$$|V_{(A)}| = 1.$$

Case (B): Diagonalizable matrices with two different eigenvalues $\lambda, \mu \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}.$$

From the Jordan canonical form and Theorem 2.7 we see that $m_A = p_A$, i.e., all the matrices from this case are non-derogatory. This means that matrix A generates a subring of dimension 2. As every matrix in the subring $\langle A \rangle_1$ is clearly diagonal, and the space of all diagonal matrices is of dimension 2, the ring $\langle A \rangle_1$ is precisely the ring of diagonal matrices. So, the general form of matrix B from the subring $\langle A \rangle_1$ is

$$B = \begin{bmatrix} a & \\ & b \end{bmatrix}, \text{where } a \text{ and } b \text{ are arbitrary from } GF(p). \tag{4.3}$$

Obviously, if $a = b$ such a matrix will generate a subring of type (A). Matrix B is a generator of the subring $\langle A \rangle_1$ if and only if the minimal polynomial of B is of the same degree as the degree of the minimal polynomial of A and this is 2. From (4.3) we see that the degree of minimal polynomial of B will be 2 if and only if a and b are different. So, the number of generators of $\langle A \rangle_1$ is $p(p-1)$, and these matrices will be compressed into one point in $\Lambda^1(\mathcal{M}_2(GF(p)))$.

Using Proposition 4.3 we will now calculate $|V_{(B)}|$. Let us prove that the assumption of the proposition is fulfilled. Let Y be a arbitrary matrix of type (B). This means that there exists an invertible matrix S such that

$$SYS^{-1} = \begin{bmatrix} \widehat{\lambda} & \\ & \widehat{\mu} \end{bmatrix} = \widehat{A}$$

By equation (4.3) we know that the subring $\langle \widehat{A} \rangle_1 = \langle A \rangle_1$. Hence,

$$\langle Y \rangle_1 = \langle S^{-1}\widehat{A}S \rangle_1 = S^{-1}\langle \widehat{A} \rangle_1 S = S^{-1}\langle A \rangle_1 S = \langle S^{-1}AS \rangle_1,$$

i.e.,

$$S^{-1}AS \in \langle Y \rangle_1 \cap \mathcal{O}(A).$$

This proves that $\mathcal{O}(A)$ intersects every vertex of type (B).

As matrix A is non-derogatory we know from Theorem 2.12 that

$$\mathscr{C}(A) = \langle A \rangle_1 = \left\{ \begin{bmatrix} a & \\ & b \end{bmatrix} : a, b \in GF(p) \right\}. \tag{4.4}$$

A matrix from $\mathscr{C}(A)$ is invertible if and only if $a \neq 0$ and $b \neq 0$. So,

$$|\mathscr{C}(A) \cap GL_2(GF(p))| = (p-1)^2. \tag{4.5}$$

To compute ω_A let $M \in \langle A \rangle_1 \cap \mathcal{O}(A)$. From (4.3) we know that

$$M = \begin{bmatrix} a & \\ & b \end{bmatrix},$$

and since M is similar to A, we get $\{a, b\} = \{\lambda, \mu\}$. This means that (a, b) is a permutation of (λ, μ). Hence,

$$\omega_A = |\langle A \rangle_1 \cap \mathcal{O}(A)| = 2! = 2.$$

By the Proposition 4.3 we conclude that the number of vertices obtained from matrices of type (B) is equal to

$$|V_{(B)}| = \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_2(GF(p))|}{|\mathscr{C}(A) \cap GL_2(GF(p))| \cdot \omega_A} = \frac{(p^2-1)(p^2-p)}{(p-1)^2 \cdot 2} = \frac{1}{2}(p+1)p. \tag{4.6}$$

Case (C): Non-diagonalizable matrices with a double eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

From the Jordan form we can see that

$$m_A(x) = p_A(x), \tag{4.7}$$

which means that

$$\dim\langle A \rangle_1 = \deg(m_A) = 2.$$

We will use this fact to find general form of an element of the subring $\langle A \rangle_1$. Namely,

$$\langle A \rangle_1 = \mathrm{Lin}\{I, A\} = \mathrm{Lin}\{I, A - \lambda I\} = \mathrm{Lin}\{I, E_{1,2}\}.$$

As matrices I and $E_{1,2}$ are linearly independent, they form a basis of the subring $\langle A \rangle_1$, so we have

$$\langle A \rangle_1 = \left\{ \begin{bmatrix} a & b \\ & a \end{bmatrix} : a, b \in GF(p) \right\}. \tag{4.8}$$

Next, we find the generators of $\langle A \rangle_1$. Let $B \in \langle A \rangle_1$ be arbitrary. Obviously, $B = \left[\begin{smallmatrix} a & b \\ & a \end{smallmatrix}\right]$ and $\langle B \rangle_1 \subseteq \langle A \rangle_1$. Taking into account that $\langle B \rangle_1 = \langle B - aI \rangle_1$ we have

$$\langle B \rangle_1 = \mathrm{Lin}\{I, B - aI\} = \mathrm{Lin}\left\{ I, \begin{bmatrix} 0 & b \\ & 0 \end{bmatrix} \right\}.$$

So, B will be a generator of $\langle A \rangle_1$ if and only if $b \neq 0$. We conclude that out of p^2 elements of $\langle A \rangle_1$ there are $p(p-1)$ generators of $\langle A \rangle_1$.

As in case (B), we now show that the condition of Proposition 4.3 is fulfilled. Let Y be an arbitrary maatrix of type (C). This means that there exists an invertible matrix S such that

$$SYS^{-1} = \begin{bmatrix} \widehat{\lambda} & 1 \\ 0 & \widehat{\lambda} \end{bmatrix} = \widehat{A}.$$

Using equation (4.8) we have $\langle A \rangle_1 = \langle \widehat{A} \rangle_1$, hence

$$\langle Y \rangle_1 = \langle S^{-1} \widehat{A} S \rangle_1 = S^{-1} \langle \widehat{A} \rangle_1 S = S^{-1} \langle A \rangle_1 S = \langle S^{-1} A S \rangle_1.$$

Obviously, this implies that $\mathcal{O}(A)$ intersects subring $\langle Y\rangle_1$, which means that condition of Proposition 4.3 is fulfilled.

From (4.7) we see that matrix A is non-derogatory, which means that

$$\mathscr{C}(A) = \langle A\rangle_1.$$

A matrix from $\mathscr{C}(A)$ is invertible if and only if $a \neq 0$. So,

$$|\mathscr{C}(A) \cap GL_2(GF(p))| = (p-1)\cdot p = (p-1)p. \tag{4.9}$$

Next, we compute ω_A. Let $M \in \langle A\rangle_1 \cap \mathcal{O}(A)$. From (4.8) we know that

$$M = \begin{bmatrix} a & b \\ & a \end{bmatrix}.$$

Since M is similar to A we get $a = \lambda$ and M has the same degree of minimal polynomial as A, which is equivalent to $b \neq 0$. Combining the two conditions, we get

$$\omega_A = |\langle A\rangle_1 \cap \mathcal{O}(A)| = 1\cdot(p-1) = (p-1).$$

By Proposition 4.3 we obtain that the number of vertices of type (C) is equal to

$$|V_{(C)}| = \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A)\cap GL_3(GF(p))|\cdot\omega_A} = \frac{(p^2-1)(p^2-p)}{(p-1)p\cdot(p-1)} = p+1. \tag{4.10}$$

Case (D): Matrices with no eigenvalues in the field $GF(p)$, i.e., matrices whose characteristic polynomial is irreducible over $GF(p)$. Such matrices have two different eigenvalues in algebraic closure of $GF(p)$.

Let $q \in GF(p)[x]$ be a monic irreducible polynomial of degree 2 and write it in the form

$$q(x) = x^2 + a_1x + a_0. \tag{4.11}$$

Obviously, $a_0 \neq 0$, otherwise it can be factorized as $x(x+a_1)$. For polynomial q we can construct its companion matrix as

$$A = \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix}. \tag{4.12}$$

For this matrix the characteristic polynomial is exactly $p_A = q$. Note that any matrix with characteristic polynomial p_A is similar to the matrix A.

From Theorem 2.8 we infer

$$m_A(x) = p_A(x), \tag{4.13}$$

i.e., all matrices of the case (D) are non-derogatory. This means that

$$\mathscr{C}(A) = \langle A\rangle_1. \tag{4.14}$$

Obviously, m_A is an irreducible polynomial, so it follows from [26, Theorem 4.5.11] that the ideal $(m_A(x))$ is a maximal ideal of $GF(p)[x]$. By Theorem 4.4.2 from the same book the quotient ring $GF(p)[x]/(m_A(x))$ is a field.

Define the mapping

$$\varphi : GF(p)[x] \mapsto \langle A\rangle_1,$$

by

$$\varphi(s) = s(A).$$

Then φ is a ring homomorphism and

$$\operatorname{Ker}\varphi = (m_A(x)) = m_A(x) \cdot GF(p)[x].$$

Homomorphism φ is obviously surjective so the first isomorphism theorem implies

$$\langle A\rangle_1 \cong GF(p)[x]/(m_A(x)). \tag{4.15}$$

Combining (4.14) and (4.15) we conclude that $\mathscr{C}(A)$ is a field, so we easily detect invertible elements in $\mathscr{C}(A)$ as a non-zero matrices, i.e.,

$$|\mathscr{C}(A) \cap GL_2(GF(p))| = p^2 - 1.$$

As $\dim\langle A\rangle_1 = \deg(m_A) = 2$, we see that the cardinality of the subring $\langle A\rangle_1$ is p^2 as well as the field on the right side. So,

$$\langle A\rangle_1 \cong GF(p^2).$$

The only subfield of $GF(p^2)$, and hence the only subring of $\langle A\rangle_1$, is isomorphic to $GF(p)$. So, the number of generators of $\langle A\rangle_1$ is $p^2 - p$.

In this case we will not rely on Proposition 4.3 but we will calculate the number of vertices in a different way. First, we calculate the size of the orbit $\mathcal{O}(A)$. By Proposition 2.23 we have

$$|\mathcal{O}(A)| = \frac{|GL_2(GF(p))|}{|\mathscr{C}(A) \cap GL_2(GF(p))|} = \frac{(p^2-1)(p^2-p)}{p^2-1} = p^2 - p.$$

From the above we see that orbit of every matrix of type (D) contains companion matrix of an irreducible polynomial. We claim that it contains exactly one companion matrix. To prove it, suppose C_1 and C_2 are companion matrices of two monic irreducible polynomials p_1 and p_2 of degree 2, in the same orbit. As C_1 and C_2 are from the same orbit, they are similar, so they have the same characteristic polynomial, i.e., $p_1 = p_{C_1} = p_{C_2} = p_2$. This is equivalent to $C_1 = C_2$, which proves our claim.

We conclude that the number of orbits of matrices of type (D) is equal to the number of monic irreducible polynomials of degree 2, which is equal to $\frac{p^2-p}{2}$, see [33, Theorem 3.25]. Hence, the number of matrices of type (D) is equal to

$$\frac{p^2-p}{2} \cdot |\mathcal{O}(A)| = \frac{p^2-p}{2} \cdot (p^2-p) = \frac{(p^2-p)^2}{2}.$$

If we divide this number by the number of generators of the subring of type (D), calculated above, we get the number of vertices of type (D), i.e.,

$$|V_{(D)}| = \frac{(p^2-p)^2}{2(p^2-p)} = \frac{1}{2}(p^2-p). \tag{4.16}$$

Although we do not need ω_A, as in previous cases, we calculate it anyway. Let B be the matrix from the subring $\langle A\rangle_1$ similar to A. Matrices are similar if and only if there exists an invertible matrix S such that $B = SAS^{-1}$. In this case the conjugation $\pi : \langle A\rangle_1 \mapsto \langle A\rangle_1$ defined as $\pi(X) = SXS^{-1}$ is a field isomorphism with $\pi(A) = B$. On the other hand, if ϕ is an automorphism of $\langle A\rangle_1$ then $\phi(A)$ has the same minimal polynomial as A. Since m_A is irreducible, this means that $\phi(A)$ is similar to A. Hence,

$$\omega_A = \left|\{\phi(A) : \phi \in \mathrm{Aut}(\langle A\rangle_1)\}\right| = \left|\mathrm{Aut}(GF(p^2))\right|.$$

From [33, Theorem 2.21] we see that $\omega_A = 2$. Note that the cardinality of the set of generators of a subring of type (D) is equal to the product of the number of orbits and ω_A, i.e, $p^2 - p = \frac{p^2-p}{2} \cdot 2$, which proves that every subring of type (D) intersects every orbit. This means that the assumption of the Proposition 4.3 actually holds for case (D) as well.

In the Table 4.1 we summarize the results from cases (A) – (D), to have a global overview of the compression.

Table 4.1: Vertices of $\Lambda^1(\mathcal{M}_2(GF(p)))$.

CASE	Number of vertices	Number of matrices compressed	$\dim\langle A\rangle_1$
(A)	1	p	1
(B)	$\frac{1}{2}(p+1)p$	$p(p-1)$	2
(C)	$p+1$	$p(p-1)$	2
(D)	$\frac{1}{2}(p^2-p)$	p^2-p	2

Note that now we can do a quick check if the numbers in Table 4.1 are correct. We first calculate the number of matrices of each type and the sum of all those numbers should be equal to the number of all matrices, which is p^4. The number of matrices for each case is the product of the number of vertices and the number of matrices compressed into one vertex. We have p matrices of type (A), $\frac{1}{2}p^4 - \frac{1}{2}p^2$ matrices of type (B), $p^3 - p$ matrices of type (C) and $\frac{1}{2}p^4 - p^3 + \frac{1}{2}p^2$ matrices of type (D). The sum of this numbers is exactly p^4.

Before we prove an important proposition, which will help us finish the construction of $\Lambda^1(\mathcal{M}_2(GF(p)))$ recall from graph theory that we denote by K_n the complete graph on n vertices without any loops and by K_n° the complete graph on n vertices with all the loops. If G and H are two graphs we denote by $G \cup H$ their disjoint union, by tG a union of t

copies of G and by $G \vee H$ their join, i.e. the graph with $V(G \vee H) = V(G) \cup V(H)$ and $E(G \vee H) = E(G) \cup E(H) \cup \{\{a,b\} \mid a \in V(G), b \in V(H)\}$.

Proposition 4.4. *Let n be an arbitrary positive integer. Suppose u and v are two vertices which correspond to two non-derogatory matrices A and B from $\mathcal{M}_n(GF(p))$, respectively. There exists an edge between u and v if and only if $u = v$, i. e., the edge is a loop.*

Proof. If there is an edge between u and v, that means that $AB = BA$. Since A is non-derogatory it holds that $\langle A \rangle_1 = \mathscr{C}(A)$. Since B commutes with A, it follows that B belongs to $\langle A \rangle_1$, so $\langle B \rangle_1 \subseteq \langle A \rangle_1$. Similarly, $\langle A \rangle_1 \subseteq \langle B \rangle_1$, so we have $\langle B \rangle_1 = \langle A \rangle_1$ which means $u = v$. □

Note that all vertices of the compressed commuting graph of $\mathcal{M}_2(GF(p))$, except the one created by compression of the subring of scalar matrices, are represented by non-derogatory matrices. From Proposition 4.4 we conclude that there are no edges between vertices of type (B), (C) and (D) except loops and that the vertex created by compression of the subring of scalar matrices is connected by an edge with itself and with all the other $\frac{1}{2}(p+1)p$ vertices of type (B), $p+1$ vertices of type (C) and $\frac{1}{2}(p^2-1)$ vertices of type (D). This proves the following theorem.

Theorem 4.5. *Let p be a prime number. Then the unital compressed commuting graph of the ring $\mathcal{M}_2(GF(p))$ is a star graph with p^2+p+1 leaves and all the loops, i.e.,*

$$\Lambda^1(\mathcal{M}_2(GF(p))) \cong K_1^\circ \vee ((p^2+p+1)K_1^\circ). \tag{4.17}$$

We remark that Theorem 4.5 is a special case of the following more general theorem, proved in [13, Theorem 21], which describes the unital compressed commuting graph of a ring of matrices of order 2 over a general finite field. Here $d(n)$ is the number of all positive divisors of a positive integer n and $\sigma(n)$ is the sum of all positive divisors of n.

Theorem 4.6. *Let n be an integer, p a prime, and $GF(p^n)$ the field with p^n elements. Let*

$$a(n) = \begin{cases} d(n)^2 - d(n) + \sigma(n) - 1; & \text{if } p = 2 \text{ and } n \text{ is even,} \\ d(n)^2 - d(n) + \sigma(n); & \text{if } p > 2 \text{ or } n \text{ is odd,} \end{cases}$$
$$b(n) = \sum_{d|n} \frac{p^n - 1}{p^d - 1}, \quad \text{and} \quad c(n) = d(2n) - d(n).$$

Then the unital compressed commuting graph of the ring $\mathcal{M}_2(GF(p^n))$ is

$$\Lambda^1(\mathcal{M}_2(GF(p^n))) \cong K_{d(n)}^\circ \vee \left(\tfrac{p^{2n}+p^n}{2} K_{a(n)}^\circ \cup (p^n+1)K_{b(n)}^\circ \cup \tfrac{p^{2n}-p^n}{2} K_{c(n)}^\circ \right).$$

Note that in our case $n = 1$, so $a(1) = b(1) = c(1) = d(1) = 1$ and

$$\frac{p^2+p}{2} + (p+1) + \frac{p^2-p}{2} = p^2+p+1.$$

Chapter 5

Vertex set of $\Lambda^1(\mathcal{M}_3(GF(p)))$

Similarly as in the case of 2×2 matrices the problem of describing the vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$ will be divided into the several cases depending on how the characteristic polynomial of a matrix splits over the field $GF(p)$.

Case (A): Diagonalizable matrices with a triple eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{bmatrix}.$$

Case (B): Diagonalizable matrices with two different eigenvalues $\lambda, \mu \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix}.$$

Case (C): Diagonalizable matrices with three different eigenvalues $\lambda, \mu, \nu \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{bmatrix}.$$

Further cases consist of non-diagonalizable matrices.
Case (D): Matrices with a triple eigenvalue $\lambda \in GF(p)$ with minimal polynomial $(x-\lambda)^3$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{bmatrix}.$$

Case (E): Matrices with a triple eigenvalue $\lambda \in GF(p)$ with minimal polynomial $(x-\lambda)^2$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{bmatrix}.$$

Case (F): Matrices with two different eigenvalues $\lambda, \mu \in GF(p)$ with minimal polynomial $(x-\lambda)^2(x-\mu)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{bmatrix}.$$

Case (G): Matrices whose characteristic polynomial is irreducible over $GF(p)$, i.e., with no eigenvalues in the field $GF(p)$.
Case (H): Matrices whose characteristic polynomial is of the form $p(x) = (x-\lambda)(x^2+a_1x+a_0)$ where the second factor is irreducible over $GF(p)$.

Proposition 5.1. *Suppose A and B are two matrices from $\mathcal{M}_3(GF(p))$. If $\langle A\rangle_1 = \langle B\rangle_1$ then A and B are of the same type.*

Proof. First note that $\deg m_A = \deg m_B$. We denote this degree by d. As $\langle A\rangle_1 = \langle B\rangle_1$ we know that there exist polynomials q and r such that $B = q(A)$ and $A = r(B)$. This implies that matrices A and B have the same number of distinct eigenvalues in $GF(p)$. We will denote this number by e. Note that $0 \leq e \leq d \leq 3$. Now, we consider the cases based on the values of d and e.

Note that the pair $(d, e) = (1, 0)$ is not possible as linear polynomial always has a zero in the field, i.e., if $d = 1$ then $e = 1$. Furthermore, the pair $(d, e) = (2, 0)$ is not possible because it would mean that the characteristic polynomial has a double zero λ_1. Since this is a zero of minimal polynomial it is an element of $GF(p^2) \setminus GF(p)$. But then the second zero λ_2 of the minimal polynomial must be double as well, which is not possible.

If $(d, e) = (1, 1)$ then matrices A and B are of type (A). Similarly, if $(d, e) = (2, 1)$ they are of type (E), if $(d, e) = (2, 2)$ they are of type (B), if $(d, e) = (3, 0)$ they are of type (G), if $(d, e) = (3, 2)$ they are of type (F), if $(d, e) = (3, 3)$ they are of type (C). Finally, if $(d, e) = (3, 1)$ we distinguish two subcases. If matrix A has all eigenvalues in $GF(p)$ then so does B because $B = q(A)$. In this case both matrices are of type (D). On the other hand, if A has an eigenvalue $\alpha \notin GF(p)$ then so does B, because $\alpha = r(\beta)$ for some eigenvalue β of B and clearly $\beta \notin GF(p)$. So, both matrices are of type (H). □

Now, as a first step in the description of the compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$ we will calculate the number of vertices of the compressed commuting graph for each case separately. Note that from Proposition 5.1 we know that compression is possible only within the certain type.

Case (A): Diagonalizable matrices with a triple eigenvalue $\lambda \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}.$$

The minimal polynomial of matrix A is $m_A(x) = x - \lambda$, which means that $\langle A \rangle_1 = \mathrm{Lin}\{I\}$, i.e., the subring $\langle A \rangle_1$ consists only of p scalar matrices. Every scalar matrix from the subring is a generator of the subring. In other words all the matrices from the subring will be compressed to one vertex in $\Lambda^1(\mathcal{M}_3(GF(p)))$.

Let B be a matrix from $\mathcal{M}_3(GF(p))$ similar to $A = \lambda I$. This means that there exists an invertible matrix S such that

$$B = S^{-1} \cdot A \cdot S = S^{-1} \cdot \lambda I \cdot S = \lambda S^{-1} \cdot I \cdot S = \lambda S^{-1} \cdot S = \lambda I = A.$$

So, there are no matrices similar to $A = \alpha I$ apart from A itself, and the subring $\langle A \rangle_1$ is unique subring of type (A), hence, in the $\Lambda^1(\mathcal{M}_3(GF(p)))$ there is only one vertex of type (A), i.e.,

$$|V_{(A)}| = 1.$$

Case (B): Diagonalizable matrices with two different eigenvalues $\lambda, \mu \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix}.$$

The minimal polynomial of matrix A is $m_A(x) = (x - \lambda)(x - \mu)$, which is of degree 2, so we know that $\dim \langle A \rangle_1 = 2$. This fact can be used to find the general form of an element from the subring $\langle A \rangle_1$. Namely,

$$\begin{aligned} \langle A \rangle_1 &= \{p(A) : p \in \mathbb{Z}[x]\} = \{p(A) : p \in GF(p)[x]\} \\ &= \mathrm{Lin}\{I, A\} = \mathrm{Lin}\{I, A - \mu I\} \\ &= \mathrm{Lin}\{I, (\lambda - \mu)E_{11}\} = \mathrm{Lin}\{E_{11}, E_{22} + E_{33}\} \\ &= \left\{ \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \beta \end{bmatrix} : \alpha, \beta \in GF(p) \right\}. \end{aligned} \tag{5.1}$$

Now we calculate the number of generators of $\langle A \rangle_1$. Let a matrix $B \in \langle A \rangle_1$ be arbitrary. Note that B is a generator if and only if its minimal polynomial is of degree equal to the degree of the minimal polynomial of matrix A, which is equal to 2. As the general form of B is visible from (5.1), B is a generator if and only if $\beta \neq \alpha$. So, the number of generators of $\langle A \rangle_1$ is $p(p-1)$. These matrices will be compressed into one vertex in the $\Lambda^1(\mathcal{M}_3(GF(p)))$. On the other hand, if $\beta = \alpha$ then $\langle B \rangle_1$ is the ring of scalar matrices, which is the only proper subring of $\langle A \rangle_1$ and was discussed in case (A).

To calculate the cardinality of $V_{(B)}$ we will use the same strategy that was used in the case of matrices of order 2, so we first show that the assumption of Proposition 4.3 is satisfied. Let Y be an arbitrary matrix of type (B). This means that there exists an invertible matrix S such that

$$SYS^{-1} = \begin{bmatrix} \widehat{\lambda} & & \\ & \widehat{\mu} & \\ & & \widehat{\mu} \end{bmatrix} = \widehat{A}$$

By equation (5.1) we know that the subring $\langle \widehat{A} \rangle_1 = \langle A \rangle_1$. Hence,

$$\langle Y \rangle_1 = \langle S^{-1}\widehat{A}S \rangle_1 = S^{-1}\langle \widehat{A} \rangle_1 S = S^{-1}\langle A \rangle_1 S = \langle S^{-1}AS \rangle_1, \tag{5.2}$$

i.e.,

$$S^{-1}AS \in \langle Y \rangle_1 \cap \mathcal{O}(A).$$

So the assumption is satisfied.

Next, we determine the centralizer $\mathscr{C}(A)$. A matrix $X = \left[\begin{smallmatrix} a & b & c \\ d & e & f \\ g & h & i \end{smallmatrix}\right]$ is in $\mathscr{C}(A)$ if and only if

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \cdot \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix} = \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix} \cdot \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix},$$

$$\begin{bmatrix} a\lambda & b\mu & c\mu \\ d\lambda & e\mu & f\mu \\ g\lambda & h\mu & i\mu \end{bmatrix} = \begin{bmatrix} \lambda a & \lambda b & \lambda c \\ \mu d & \mu e & \mu f \\ \mu g & \mu h & \mu i \end{bmatrix}.$$

This matrix equation is equivalent to the system of equations (over the field $GF(p)$)

$$\begin{cases} b\mu = \lambda b, \\ c\mu = \lambda c, \\ d\lambda = \mu d, \\ g\lambda = \mu g. \end{cases}$$

Taking into account that $\mu \neq \lambda$, the solution is $b = c = d = g = 0$ while a, e, f, h, i are arbitrary elements of the field $GF(p)$. So, the centralizer of the matrix A is

$$\mathscr{C}(A) = \left\{ \begin{bmatrix} a & & \\ & e & f \\ & h & i \end{bmatrix} : a, e, f, h, i \in GF(p) \right\}. \tag{5.3}$$

From Proposition 2.21 we know that $|GL_3(GF(p))| = (p^3 - 1) \cdot (p^3 - p) \cdot (p^3 - p^2)$. Now we will calculate the number of invertible matrices in the centralizer of A. Matrix $\left[\begin{smallmatrix} a & & \\ & e & f \\ & h & i \end{smallmatrix}\right]$ is invertible if and only if $a \neq 0$ and matrix $\left[\begin{smallmatrix} e & f \\ h & i \end{smallmatrix}\right]$ is invertible, hence

$$|\mathscr{C}(A) \cap GL_3(GF(p))| = |GL_1(GF(p))| \cdot |GL_2(GF(p))| = (p-1)(p^2-1)(p^2-p). \tag{5.4}$$

We will now prove that we have $\omega_A = 1$. Let $M \in \langle A\rangle_1 \cap \mathcal{O}(A)$ be arbitrary. As $M \in \langle A\rangle_1$ we infer from the equation (5.1) that $M = \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \beta \end{bmatrix}$ for some $\alpha, \beta \in GF(p)$. Since $M \in \mathcal{O}(A)$, it must have the same eigenvalues with the same algebraic multiplicities as matrix A. So $\alpha = \lambda$ and $\beta = \mu$, i.e., $M = A$, which proves our claim. By Proposition 4.3 the number of vertices of type (B) is

$$|V_{(B)}| = \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A) \cap GL_3(GF(p))| \cdot \omega_A} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)(p^2-1)(p^2-p)\cdot 1} = (p^2+p+1)p^2.$$

Case (C): Diagonalizable matrices with three different eigenvalues $\lambda, \mu, \nu \in GF(p)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{bmatrix}.$$

Note that in this case p must be greater then or equal to 3 because if $p = 2$ a matrix cannot have three different eigenvalues in $GF(p)$.

From the Jordan canonical form we see that $m_A = p_A$, i.e., all the matrices from this case are non-derogatory. This means that matrix A generates subring of dimension 3. As every matrix in subring $\langle A\rangle_1$ is clearly diagonal, and the space of all diagonal matrices is of the dimension 3, the ring $\langle A\rangle_1$ is precisely the ring of diagonal matrices. So, the general form of the matrix B from the subring $\langle A\rangle_1$ is

$$B = \begin{bmatrix} a & & \\ & b & \\ & & c \end{bmatrix}, \text{where } a, b \text{ and } c \text{ are arbitrary from } GF(p). \tag{5.5}$$

Obviously, if $a = b = c$ such a matrix generates subring of type (A). If $b = c \neq a$, $a = b \neq c$ or $a = c \neq b$ matrix B generates a subring of type (B). The matrix $B \in \langle A\rangle_1$ is a generator of subring $\langle A\rangle_1$ if and only if the minimal polynomial of B is of degree the same as degree of minimal polynomial of A and this is 3. From (5.5) we see that degree of minimal polynomial will be 3 if and only if a, b and c are different. So, the number of generators is $p(p-1)(p-2)$. These matrices will be compressed into one vertex in the $\Lambda^1(\mathcal{M}_3(GF(p)))$.

Note that subring from equation (5.5) does not depend on the exact values of λ, μ and ν. This implies that we can use the same argument as in case (B) (see equation (5.2)) and conclude that the orbit of A intersects every vertex of type (C). This means that the assumption of Proposition 4.3 is satisfied.

As matrix A is non-derogatory we know that

$$\mathscr{C}(A) = \langle A\rangle_1 = \left\{ \begin{bmatrix} a & & \\ & b & \\ & & c \end{bmatrix} : a, b, c \in GF(p) \right\}. \tag{5.6}$$

Matrix from $\mathscr{C}(A)$ is invertible if and only if $a \neq 0$, $b \neq 0$ and $c \neq 0$. So,

$$|\mathscr{C}(A) \cap GL_3(GF(p))| = (p-1)^3. \tag{5.7}$$

Note that the subring from equation (5.5) is independent of the specific values of λ, μ and ν. Hence, we can use similar arguments as in case (B) to conclude that $\mathcal{O}(A)$ intersects any vertex of type (C). So, again it is sufficient to consider $\mathcal{O}(A)$ to find the number of vertices of type (C).

Let $M \in \langle A \rangle_1 \cap \mathcal{O}(A)$. From (5.5) we know that

$$M = \begin{bmatrix} a & & \\ & b & \\ & & c \end{bmatrix}$$

and since M is similar to A we get $\{a, b, c\} = \{\lambda, \mu, \nu\}$. This means that (a, b, c) is a permutation of (λ, μ, ν). Hence,

$$\omega_A = |\langle A \rangle_1 \cap \mathcal{O}(A)| = 3! = 6.$$

By Proposition 4.3 we conclude that the number of vertices of type (C) is equal to

$$\begin{aligned} |V_{(C)}| &= \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A) \cap GL_3(GF(p))| \cdot \omega_A} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)^3 \cdot 6} \\ &= \frac{1}{6}(p^2+p+1)p^3(p+1). \end{aligned} \tag{5.8}$$

Case (D): Matrices with a triple eigenvalue $\lambda \in GF(p)$ with minimal polynomial $(x-\lambda)^3$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{bmatrix}.$$

From the Jordan form we can see that

$$m_A(x) = p_A(x) \tag{5.9}$$

which means that

$$\dim\langle A \rangle_1 = \deg(m_A) = 3.$$

We use this fact to find the general form of an element of the subring $\langle A \rangle_1$. Namely,

$$\begin{aligned} \langle A \rangle_1 &= \mathrm{Lin}\{I, A, A^2\} \\ &= \mathrm{Lin}\{I, A-\lambda I, A^2-\lambda^2 I\} \\ &= \mathrm{Lin}\{I, E_{1,2}+E_{2,3}, A^2-\lambda^2 I - 2\lambda(E_{1,2}+E_{2,3})\} \\ &= \mathrm{Lin}\{I, E_{1,2}+E_{2,3}, E_{1,3}\} \end{aligned}$$

As these matrices are linearly independent, they form a basis of the subring, so we have

$$\langle A\rangle_1 = \left\{ \begin{bmatrix} a & b & c \\ & a & b \\ & & a \end{bmatrix} : a, b, c \in GF(p) \right\}. \tag{5.10}$$

Now we determine elements of the subring $\langle A\rangle_1$ which are generators. Suppose a matrix $B \in \langle A\rangle_1$ is arbitrary. Obviously, $B = \left[\begin{smallmatrix} a & b & c \\ & a & b \\ & & a \end{smallmatrix}\right]$ and $\langle B\rangle_1 \subseteq \langle A\rangle_1$. Taking into account that

$$\langle B\rangle_1 = \langle B - aI\rangle_1$$

we have

$$\begin{aligned} \langle B\rangle_1 &= \mathrm{Lin}\{I, B - aI, (B - aI)^2\} \\ &= \mathrm{Lin}\left\{ I, \begin{bmatrix} 0 & b & c \\ & 0 & b \\ & & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & b^2 \\ & 0 & 0 \\ & & 0 \end{bmatrix} \right\} \end{aligned}$$

So, B is a generator of $\langle A\rangle_1$ if and only if $b \neq 0$. We conclude that out of p^3 elements of $\langle A\rangle_1$ there are $p(p-1)p = p^2(p-1)$ generators of $\langle A\rangle_1$. If $b = 0$ then we have two possibilities:

(i) $c = 0$, in which case $\langle B\rangle_1$ is of dimension 1 or

(ii) $c \neq 0$, in which $\langle B\rangle_1$ is of dimension 2.

Once again the subring from (5.10) does not depend on the value of λ, so, as in previous cases, the assumption of Proposition 4.3 is fulfilled. From (5.9) we see that matrix A is non-derogatory, which means that

$$\mathscr{C}(A) = \langle A\rangle_1. \tag{5.11}$$

Matrix from $\mathscr{C}(A)$ is invertible if and only if $a \neq 0$. So,

$$|\mathscr{C}(A) \cap GL_3(GF(p))| = (p-1) \cdot p \cdot p = (p-1)p^2. \tag{5.12}$$

Let $M \in \langle A\rangle_1 \cap \mathcal{O}(A)$. From (5.10) we know that

$$M = \begin{bmatrix} a & b & c \\ & a & b \\ & & a \end{bmatrix}.$$

Since M is similar to A we get $a = \lambda$ and M has the same degree of minimal polynomial as A, which is equivalent to $b \neq 0$. Note that, as soon as $a = \lambda$ and $b \neq 0$, matrix M has minimal polynomial of degree 3 equal to the minimal polynomial of A, hence, M is automatically similar to A. Combining the two conditions, we get

$$\omega_A = |\langle A\rangle_1 \cap \mathcal{O}(A)| = 1 \cdot (p-1) \cdot p = (p-1)p.$$

We finish the case by counting the number of vertices of type (D), using Proposition 4.3. We get

$$|V_{(D)}| = \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A) \cap GL_3(GF(p))| \cdot \omega_A} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)p^2 \cdot (p-1)p} \\ = (p^3-1)(p+1). \tag{5.13}$$

Case (E): Matrices with a triple eigenvalue $\lambda \in GF(p)$ with minimal polynomial $(x-\lambda)^2$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{bmatrix}.$$

From the Jordan form we can see that $p_A(x) = (x-\lambda)^3$ and $m_A(x) = (x-\lambda)^2$ which gives us $\dim\langle A\rangle_1 = \deg(m_A) = 2$. So,

$$\langle A\rangle_1 = \langle A - \lambda I\rangle_1 = \mathrm{Lin}\{I, A-\lambda I\} = \mathrm{Lin}\{I, E_{1,2}\}.$$

This calculation gives us

$$\langle A\rangle_1 = \left\{ \begin{bmatrix} a & b & \\ & a & \\ & & a \end{bmatrix} : a, b \in GF(p) \right\}. \tag{5.14}$$

Next, we calculate the number of generators of $\langle A\rangle_1$. Let a matrix $B \in \langle A\rangle_1$ be arbitrary. Note that B is a generator if and only if its minimal polynomial is of degree 2. As general form of B is visible from (5.14), B will be a generator if and only if $b \neq 0$. So, the number of generators of $\langle A\rangle_1$ is $p(p-1)$. On the other hand, if $b = 0$ then $\langle B\rangle_1$ is the ring of scalar matrices, which is the only proper subring of $\langle A\rangle_1$.

Note that again the subring from (5.14) does not depend on the specific value of λ, so the assumption of Proposition 4.3 is satisfied. We now calculate $\mathscr{C}(A)$, the centralizer of matrix A. Knowing that

$$\mathscr{C}(A) = \mathscr{C}(A - \lambda I),$$

let $X = \left[\begin{smallmatrix} a & b & c \\ d & e & f \\ g & h & i \end{smallmatrix}\right] \in \mathscr{C}(A - \lambda I)$ be arbitrary. We have

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$
$$\begin{bmatrix} 0 & a & 0 \\ 0 & d & 0 \\ 0 & g & 0 \end{bmatrix} = \begin{bmatrix} d & e & f \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

which is equivalent to

$$\begin{cases} d = 0, \\ a = e, \\ f = 0, \\ g = 0, \end{cases}$$

i.e., $X = \begin{bmatrix} a & b & c \\ 0 & a & 0 \\ 0 & h & i \end{bmatrix}$. So,

$$\mathscr{C}(A) = \left\{ \begin{bmatrix} a & b & c \\ 0 & a & 0 \\ 0 & h & i \end{bmatrix} : a, b, c, h, i \in GF(p) \right\}. \tag{5.15}$$

We proceed similarly as in previous cases. A matrix from $\mathscr{C}(A)$ is invertible if and only if $a \neq 0$ and $i \neq 0$. So,

$$\big|\mathscr{C}(A) \cap GL_3(GF(p))\big| = (p-1) \cdot p \cdot p \cdot p \cdot (p-1) = (p-1)^2 p^3.$$

Let $M \in \langle A \rangle_1 \cap \mathcal{O}(A)$. From (5.14) we know that

$$M = \begin{bmatrix} a & b & \\ & a & \\ & & a \end{bmatrix}$$

and since M is similar to A, they have the same eigenvalue, i.e., $a = \lambda$, and the same degree of minimal polynomial, so $b \neq 0$. Therefore,

$$\omega_A = |\langle A \rangle_1 \cap \mathcal{O}(A)| = 1 \cdot (p-1) = p - 1.$$

We conclude by Proposition 4.3 that the number of vertices of type (E) is equal to

$$\begin{aligned} |V_{(E)}| :&= \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A) \cap GL_3(GF(p))| \cdot \omega_A} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)^2 p^3 \cdot (p-1)} \\ &= (p^2+p+1)(p+1). \end{aligned} \tag{5.16}$$

Case (F): Matrices with two different eigenvalues $\lambda, \mu \in GF(p)$ with minimal polynomial $(x-\lambda)^2(x-\mu)$, i.e., similar to

$$A = \begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{bmatrix}.$$

From the Jordan canonical form we can see that

$$m_A(x) = p_A(x), \tag{5.17}$$

which gives us $\dim\langle A\rangle_1 = \deg(m_A) = 3$. Knowing the dimension, it is easy to find the form of a general element of the subring

$$\begin{aligned}
\langle A\rangle_1 &= \langle A-\lambda I\rangle_1 = \operatorname{Lin}\{I, A-\lambda I, (A-\lambda I)^2\} \\
&= \operatorname{Lin}\left\{I, \begin{bmatrix}0 & 1 & \\ & 0 & \\ & & \mu-\lambda\end{bmatrix}, \begin{bmatrix}0 & 1 & \\ & 0 & \\ & & \mu-\lambda\end{bmatrix}^2\right\} \\
&= \operatorname{Lin}\left\{I, \begin{bmatrix}0 & 1 & \\ & 0 & \\ & & \mu-\lambda\end{bmatrix}, \begin{bmatrix}0 & 0 & \\ & 0 & \\ & & (\mu-\lambda)^2\end{bmatrix}\right\} \\
&= \operatorname{Lin}\left\{I, \begin{bmatrix}0 & 1 & \\ & 0 & \\ & & \mu-\lambda\end{bmatrix}, E_{3,3}\right\} \\
&= \operatorname{Lin}\left\{I - E_{3,3}, \begin{bmatrix}0 & 1 & \\ & 0 & \\ & & \mu-\lambda\end{bmatrix} - (\mu-\lambda)E_{3,3}, E_{3,3}\right\} \\
&= \operatorname{Lin}\{E_{1,1}+E_{2,2}, E_{1,2}, E_{3,3}\}
\end{aligned}$$

As the generating matrices are linearly independent, they form a basis of the subring $\langle A\rangle_1$, so

$$\langle A\rangle_1 = \left\{\begin{bmatrix}a & c & \\ & a & \\ & & b\end{bmatrix} : a,b,c \in GF(p)\right\}. \tag{5.18}$$

We now determine the generators of $\langle A\rangle_1$. Let a matrix B from $\langle A\rangle_1$ be arbitrary. Note that if $c=0$ and $b=a$ then B generates a subring of type (A); if $c=0$ and $b\neq a$ then B generates a subring of type (B) and if $c\neq 0$ and $a=b$ then B generates a subring of type (D). For all other matrices in $\langle A\rangle_1$ we have that $c\neq 0$ and $b\neq a$ so the degree of their minimal polynomial is 3, i.e., they are generators of $\langle A\rangle_1$. These two conditions imply that the number of generators is $p\cdot(p-1)\cdot(p-1) = p(p-1)^2$.

Note that the subring (5.18) does not depend on the specific values of λ and μ, so again the assumption of Proposition 4.3 is satisfied. From (5.17) we see that the matrix A is non-derogatory, which means that

$$\mathscr{C}(A) = \langle A\rangle_1, \tag{5.19}$$

and we have the general form of an element from $\langle A\rangle_1$ in (5.18). Matrix from $\mathscr{C}(A)$ is invertible if and only if $a\neq 0$ and $b\neq 0$. So,

$$|\mathscr{C}(A)\cap GL_3(GF(p))| = (p-1)\cdot(p-1)\cdot p = (p-1)^2 p. \tag{5.20}$$

Let $M\in\langle A\rangle_1\cap\mathcal{O}(A)$. From (5.18) we know that

$$M = \begin{bmatrix}a & c & \\ & a & \\ & & b\end{bmatrix}$$

and since M is similar to A they have both eigenvalues equal, i.e., $a = \lambda$ and $b = \mu$, and they have the same degree of the minimal polynomial, so $c \neq 0$. Therefore,

$$\omega_A = |\langle A\rangle_1 \cap \mathcal{O}(A)| = 1 \cdot 1 \cdot (p-1) = p-1.$$

By Proposition 4.3 we conclude that the number of vertices of type (F) is equal to

$$\begin{aligned} |V_{(F)}| &= \frac{|\mathcal{O}(A)|}{\omega_A} = \frac{|GL_3(GF(p))|}{|\mathscr{C}(A) \cap GL_3(GF(p))| \cdot \omega_A} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p-1)^2 p \cdot (p-1)} \\ &= (p^2+p+1)p^2(p+1). \end{aligned} \tag{5.21}$$

Case (G): Matrices whose characteristic polynomial is irreducible over $GF(p)$, i.e., with no eigenvalues in the field $GF(p)$.

Let q be a monic irreducible polynomial of degree 3 from $GF(p)[x]$ and write it in the form

$$q(x) = x^3 + a_2 x^2 + a_1 x + a_0. \tag{5.22}$$

Obviously, $a_0 \neq 0$, otherwise it can be factorised as $x(x^2 + a_2 x + a_1)$. For polynomial q we can construct its companion matrix as

$$A = \begin{bmatrix} 0 & & -a_0 \\ 1 & 0 & -a_1 \\ & 1 & -a_2 \end{bmatrix}. \tag{5.23}$$

For this matrix the characteristic polynomial is exactly $p_A = q$. Note that any matrix with characteristic polynomial p_A is similar to the matrix A, i.e., orbit of every matrix of type (G) contains at least one companion matrix. From Theorem 2.8 we have

$$m_A(x) = p_A(x), \tag{5.24}$$

i.e., all matrices of the case (G) are non-derogatory. This means that

$$\mathscr{C}(A) = \langle A\rangle_1. \tag{5.25}$$

As m_A is an irreducible polynomial, it follows from [26, Theorem 4.5.11] that the ideal $(m_A(x))$ is a maximal ideal of $GF(p)[x]$. By Theorem 4.4.2 from the same book the quotient ring $GF(p)[x]/(m_A(x))$ is a field. Define the mapping

$$\varphi : GF(p)[x] \mapsto \langle A\rangle_1,$$

by

$$\varphi(q) = q(A).$$

Then the mapping φ is a ring homomorphism and

$$\operatorname{Ker} \varphi = (m_A(x)) = m_A(x) \cdot GF(p)[x].$$

Homomorphism φ is obviously surjective so the first isomorphism theorem implies

$$\langle A\rangle_1 \cong GF(p)[x]/(m_A(x)). \tag{5.26}$$

As $\dim\langle A\rangle_1 = \deg(m_A) = 3$, we see that the cardinality of the subring $\langle A\rangle_1$ is p^3. So,

$$\langle A\rangle_1 \cong GF(p^3). \tag{5.27}$$

The only subfield of $GF(p^3)$, and hence the only subring of $\langle A\rangle_1$, is isomorphic to $GF(p)$. So, the number of generators of $\langle A\rangle_1$ is $p^3 - p$. Combining (5.25) and (5.26) we conclude that $\mathscr{C}(A)$ is a field, so we easily detect invertible elements in $\mathscr{C}(A)$ as non-zero matrices, so that

$$|\mathscr{C}(A) \cap GL_3(GF(p))| = p^3 - 1. \tag{5.28}$$

We continue in a slightly different way than in the previous cases because, as it turns out, the subring generated by the matrix A from equation (5.23) now depends on the choice of a_0, a_1 and a_2. Instead, we will argue similarly as in the case (D) of 2×2 matrices. From Proposition 2.23 we know that

$$|\mathcal{O}(A)| = \frac{\big|GL_3(GF(p))\big|}{\big|\mathscr{C}(A) \cap GL_3(GF(p))\big|} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p^3-1)} = (p^3-p)(p^3-p^2).$$

From above we know that the orbit of every matrix of type (G) contains a companion matrix of an irreducible polynomial. In fact, it contains exactly one companion matrix, because if C_1 and C_2 are companion matrices of two irreducible polynomials degree 3 contained in the same orbit, then C_1 is similar to C_2 which implies that $p_{C_1} = p_{C_2}$ and hence $C_1 = C_2$. So, the number of orbits in this case is the same as the number of monic irreducible polynomials of degree 3, which is equal $\frac{p^3-p}{3}$ by [33, Theorem 3.25]. This means that the number of all matrices of type (G) is equal to

$$\frac{p^3-p}{3} \cdot |\mathcal{O}(A)| = \frac{p^3-p}{3} \cdot (p^3-p)(p^3-p^2) = \frac{(p^3-p)(p^3-p)(p^3-p^2)}{3}.$$

If we divide this number by the number of generators of a subring of type (G) we get the number of vertices of type (G)

$$|V_{(G)}| = \frac{(p^3-p)(p^3-p)(p^3-p^2)}{3(p^3-p)} = \frac{(p^3-p)(p^3-p^2)}{3}. \tag{5.29}$$

Although we do not strictly need $\omega_A = |\langle A\rangle_1 \cap \mathcal{O}(A)|$ as in the previous cases, lets calculate it anyway. Let B be the matrix from the subring $\langle A\rangle_1$ such that B is similar to A. The matrices are similar if and only if there exists an invertible matrix S such that $B = SAS^{-1}$. In this case the conjugation $\pi : \langle A\rangle_1 \mapsto \langle A\rangle_1$ defined as $\pi(X) = SXS^{-1}$ is a field automorphism with

$\pi(A) = B$. On the other hand, if ϕ is an automorphism of $\langle A\rangle_1$ then $\phi(A)$ has the same minimal polynomial as A. Since m_A is irreducible this, means that $\phi(A)$ is similar to A. Hence,

$$\omega_A = \big|\{\phi(A) : \phi \in \operatorname{Aut}(\langle A\rangle_1)\}\big| = \big|\operatorname{Aut}(GF(p^3))\big|.$$

From [33, Theorem 2.21] we conclude that $\omega_A = 3$. Note that the number of generators of a subring of type (G), which is equal to $p^3 - p$, satisfies equality $p^3 - p = \frac{p^3-p}{3} \cdot \omega_A$, the product of the number of orbits and ω_A, which implies that every subring of type (G) intersects every orbit. This means that the assumption of the Proposition 4.3 actually holds in this case.

Case (H): Matrices whose characteristic polynomial is of the form

$$(x - \lambda)(x^2 + a_1x + a_0) \tag{5.30}$$

where λ, a_1 and a_0 are from the field $GF(p)$ and $p_2(x) := x^2 + a_1x + a_0$ is irreducible over $GF(p)$. This means that one eigenvalue is in $GF(p)$ and the other two are not. Such matrices have three different eigenvalues in the algebraic closure of $GF(p)$.

For every polynomial of type (5.30) we can construct a matrix as a block-diagonal combination of companion matrices of factors, namely

$$A = \begin{bmatrix} \lambda & & \\ & 0 & -a_0 \\ & 1 & -a_1 \end{bmatrix} = \left[\begin{array}{c|cc} \lambda & & \\ \hline & 0 & -a_0 \\ & 1 & -a_1 \end{array}\right] = \left[\begin{array}{c|c} \lambda & \\ \hline & X \end{array}\right]. \tag{5.31}$$

Obviously, matrix A has characteristic polynomial $p_A(x) = (x-\lambda)(x^2+a_1x+a_0)$ from equation (5.30). According to Theorem 2.8 we have

$$m_A(x) = p_A(x). \tag{5.32}$$

A consequence of the previous point is that each matrix whose characteristic polynomial is $p_A(x)$ is non-derogatory, so it is similar to A, i.e., the orbit of every matrix of type (H) contains at least one matrix of the form (5.31).

For the matrix A defined in (5.31) consider the subring

$$\langle A\rangle_1 = \{p(A) : p \in \mathbb{Z}[x]\}.$$

From (5.32) we know that $\deg m_A(x) = 3$, so we have

$$\dim\langle A\rangle_1 = 3. \tag{5.33}$$

As matrix X defined in (5.31) has characteristic polynomial $p_X(x) = p_2(x) = x^2 + a_1x + a_0$, the Cayley Hamilton theorem implies

$$X^2 + a_1X + a_0I = 0, \tag{5.34}$$

which means that

$$X^2 = -a_1 X - a_0 I. \tag{5.35}$$

Now we use (5.35) to determine the subring $\langle A \rangle_1$, namely

$$\begin{aligned}
\langle A \rangle_1 &= \mathrm{Lin}\{I, A, A^2\} \\
&= \mathrm{Lin}\left\{I, \left[\begin{array}{c|c} \lambda & \\ \hline & X \end{array}\right], \left[\begin{array}{c|c} \lambda^2 & \\ \hline & X^2 \end{array}\right]\right\} \\
&= \mathrm{Lin}\left\{I, \left[\begin{array}{c|c} \lambda & \\ \hline & X \end{array}\right], \left[\begin{array}{c|c} \lambda^2 & \\ \hline & -a_1 X - a_0 I \end{array}\right]\right\}.
\end{aligned}$$

If we replace the third matrix A^2 with the linear combination $A^2 + a_1 A + a_0 I$ we get

$$\langle A \rangle_1 = \mathrm{Lin}\left\{I, \left[\begin{array}{c|c} \lambda & \\ \hline & X \end{array}\right], \left[\begin{array}{c|c} \lambda^2 + a_1\lambda + a_0 & \\ \hline & 0 \end{array}\right]\right\}.$$

On the position $(1,1)$ of the third matrix we recognize $p_2(\lambda)$ which is a non-zero element of the field $GF(p)$ as the polynomial p_2 is irreducible. This means that the element $p_2(\lambda)$ is invertible, so we can multiply the third matrix with $p_2(\lambda)^{-1}$ and get $E_{1,1}$. So, we have

$$\langle A \rangle_1 = \mathrm{Lin}\left\{I, \left[\begin{array}{c|c} \lambda & \\ \hline & X \end{array}\right], E_{1,1}\right\}.$$

Now, we replace matrix I with $I - E_{1,1} = E_{2,2} + E_{3,3}$ and matrix A with $A - \lambda E_{1,1}$ and reorder them to get

$$\langle A \rangle_1 = \mathrm{Lin}\left\{E_{1,1}, E_{2,2} + E_{3,3}, \left[\begin{array}{c|c} 0 & \\ \hline & X \end{array}\right]\right\}. \tag{5.36}$$

Now it easy to calculate the number of generators. Let B from $\langle A \rangle_1$ be an arbitrary matrix. We have

$$B = \left[\begin{array}{c|cc} a & & \\ \hline & b & -ca_0 \\ & c & b - ca_1 \end{array}\right] \tag{5.37}$$

where a, b and c are from $GF(p)$. Matrix B is a generator of $\langle A \rangle_1$ if and only if its minimal polynomial is of degree 3. As we see, matrix B is block-diagonal matrix, so by the Theorem 2.9 the minimal polynomial of matrix B is the least common multiple of the minimal polynomials of the blocks. Let us concentrate on the lower right block. Obviously, for $c = 0$ we have a scalar matrix whose minimal polynomial is of degree 1, so for now we will consider case $c \neq 0$. In this case, the characteristic polynomial of the lower right block is

$$\begin{aligned}
p_{bI+cX}(x) &= \det \begin{bmatrix} b-x & -ca_0 \\ c & b-ca_1-x \end{bmatrix} \\
&= \det \begin{bmatrix} -(x-b) & -ca_0 \\ c & -ca_1-(x-b) \end{bmatrix} \\
&= c^2 \cdot \det \begin{bmatrix} -(x-b)c^{-1} & -a_0 \\ 1 & -a_1-(x-b)c^{-1} \end{bmatrix} \\
&= c^2 \cdot p_X((x-b)c^{-1}).
\end{aligned}$$

As matrix X has characteristic polynomial p_2, which is irreducible, for all α from $GF(p)$ it holds that

$$p_{bI+cX}(\alpha) = p_X((\alpha-b)c^{-1}) \neq 0,$$

i.e., the lower right block of matrix B has irreducible characteristic polynomial. So, its minimal polynomial is irreducible, which means that the minimal polynomial of the matrix B is of degree 3 and B generates $\langle A\rangle_1$. Hence, the number of generators of the subring $\langle A\rangle_1$ is

$$p \cdot p \cdot (p-1) = p^2(p-1).$$

For case $c = 0$, obviously, we have two cases. If $a = b$ then B is a scalar matrix, a generator of the subring of type (A), and if $a \neq b$ then B generates a subring of type (B).

As a consequence of (5.32) matrix A is non-derogatory, so from Theorem 2.12 we have

$$\mathscr{C}(A) = \langle A\rangle_1. \tag{5.38}$$

We proceed similarly as in case (G). A matrix from $\mathscr{C}(A)$ is of the form given in (5.37) and is invertible if and only if

$$\begin{vmatrix} a & & \\ & b & -ca_0 \\ & c & b-ca_1 \end{vmatrix} = a(b(b-ca_1)+c^2a_0) \neq 0.$$

This is equivalent to $a \neq 0$ and

$$b^2 - bca_1 + c^2a_0 \neq 0. \tag{5.39}$$

As the first case, we consider (5.39) under condition $c \neq 0$. When we multiply (5.39) with c^{-2} we get

$$\begin{aligned}
\left(\frac{b}{c}\right)^2 - a_1\left(\frac{b}{c}\right) + a_0 &\neq 0 \\
\left(-\frac{b}{c}\right)^2 + a_1\left(-\frac{b}{c}\right) + a_0 &\neq 0 \\
p_2\left(-\frac{b}{c}\right) &\neq 0
\end{aligned}$$

which is true for all b and $c \neq 0$ from $GF(p)$ as p_2 is an irreducible polynomial. In second case, when $c = 0$, we have $b^2 \neq 0$ so $b \neq 0$. Hence, $a \neq 0$ and at least one of b and c is non zero. So,

$$\begin{aligned}\left|\mathscr{C}(A) \cap GL_3(GF(p))\right| &= (p-1) \cdot p \cdot (p-1) + (p-1) \cdot (p-1) \cdot 1 \\ &= (p-1)^2(p+1) \\ &= (p^2-1)(p-1).\end{aligned}$$

From Proposition 2.23 we conclude that

$$|\mathcal{O}(A)| = \frac{\left|GL_3(GF(p))\right|}{\left|\mathscr{C}(A) \cap GL_3(GF(p))\right|} = \frac{(p^3-1)(p^3-p)(p^3-p^2)}{(p^2-1)(p-1)} = (p^3-1)p^3.$$

We have shown above that the orbit of every matrix of type (H) contains a matrix of the form (5.31). Similarly as in the case (G) we conclude that it contains exactly one such matrix. So, the number of orbits in this case is equal to the number of polynomials of type (5.30). To count the number of such polynomials, note that the number of possible polynomials for the first factor is p. Every polynomial from the set

$$\left\{p_\lambda(x) = x - \lambda : \lambda \in GF(p)\right\}$$

is appropriate, i.e., every element from $GF(p)$ can be the eigenvalue from the field. The number of possible polynomials for the second factor (number of monic irreducible polynomials of degree 2) is $\frac{p^2-p}{2}$, because there are p^2 monic polynomials and out of them we have $p + \frac{p(p-1)}{2}$ reducible polynomials. This means that there are in total $p \cdot \frac{p^2-p}{2}$ different polynomials suitable to be a characteristic polynomial of matrices from the case (H), hence we obtain also the same number of orbits. This implies that the number of matrices of type (H) is equal to

$$p \cdot \frac{p^2-p}{2} \cdot |\mathcal{O}(A)| = p \cdot \frac{p^2-p}{2} \cdot (p^3-1)p^3 = \frac{p^5(p-1)(p^3-1)}{2}.$$

We obtain the number of vertices of type (H) by dividing the above number by the number of generators of a subring of type (H) which is equal to $p^2(p-1)$, namely

$$|V_{(H)}| = \frac{p^5(p-1)(p^3-1)}{2p^2(p-1)} = \frac{p^3(p^3-1)}{2}. \tag{5.40}$$

We also calculate ω_A as in the previous case. From equation (5.36) we see that

$$\langle A\rangle_1 \cong GF(p) \oplus \langle X\rangle_1.$$

Similarly as in case (G) we prove that $\langle X\rangle_1 \cong GF(p^2)$ so

$$\langle A\rangle_1 \cong GF(p) \oplus GF(p^2). \tag{5.41}$$

Let $M \in \langle A \rangle_1 \cap \mathcal{O}(A)$. From (5.37) we know that

$$M = \begin{bmatrix} a & & \\ & b & -ca_0 \\ & c & b - ca_1 \end{bmatrix} = \left[\begin{array}{c|c} a & \\ \hline & Z \end{array}\right]$$

and since M is similar to A they have the same eigenvalue from the field, i.e., $a = \lambda$, and matrix Z has characteristic polynomial p_2. So, Z is similar to X, because of the irreducibility of polynomial p_2. Therefore,

$$\omega_A = |\langle A \rangle_1 \cap \mathcal{O}(A)| = \omega_X = |\langle X \rangle_1 \cap \mathcal{O}(X)|.$$

Similarly as in case (G) we conclude $\omega_A = 2$. Hence, in this case the number of generators of a subring of type (H), i.e., $p^2(p-1)$, is equal to product of the number of orbits and ω_A, i.e., $\frac{p(p^2-p)}{2} \cdot 2$. This again implies that every subring of type (H) intersects every orbit. Again, it means that the assumption of the Proposition 4.3 holds for this case, as well.

Now we summarize results from cases (A) to (H) in Table 5.1, to have a global overview of compression into vertices. We can check if the numbers in Table 5.1 are correct, namely, if we compute the scalar product of the second and third column of Table 5.1 we obtain p^9 which is exactly the cardinality of $\mathcal{M}_3(GF(p))$.

Table 5.1: Vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$.

CASE	Number of vertices	Number of matrices compressed	$\dim_{GF(p)} \langle A \rangle_1$
(A)	1	p	1
(B)	$(p^2+p+1)p^2$	$p(p-1)$	2
(C)	$\frac{1}{6}(p^2+p+1)p^3(p+1)$	$p(p-1)(p-2)$	3
(D)	$(p^3-1)(p+1)$	$p^2(p-1)$	3
(E)	$(p^2+p+1)(p+1)$	$p(p-1)$	2
(F)	$(p^2+p+1)p^2(p+1)$	$p(p-1)^2$	3
(G)	$\frac{1}{3}(p^3-p)(p^3-p^2)$	p^3-p	3
(H)	$\frac{1}{2}(p^3-1)p^3$	$p^2(p-1)$	3

Chapter 6

Neighborhoods of vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$

In this chapter we describe the neighborhood of each vertex of $\Lambda^1(\mathcal{M}_3(GF(p)))$. For a vertex v of a certain type we will calculate the number of vertices of each type that are connected to v. This will be done by investigating the centralizer of a matrix representative A of vertex v. Note that the neighborhood of the vertex v is a compressed commuting graph of the centralizer $\mathscr{C}(A)$. For the vertex v of type (Y) we will denote by $N(X,Y)$ the number of neighbors of type (X).

Suppose A is a matrix representative of a vertex v of certain type. We consider cases with respect to the type of vertex v.

Case (A): As we know that we have only one vertex of type (A) and the whole subring of scalar matrices (consists of p scalar matrices) is compressed into that one vertex, a matrix representative of the vertex v is a scalar matrix. The centralizer of a scalar matrix is the whole ring $\mathcal{M}_3(GF(p))$ so all the other vertices will be in the neighborhood of v, including v itself. Table 6.1 represents the neighborhood of v of type (A), where the number in row (X) represents the number of vertices of type (X) in the neighborhood.

Case (B): The centralizer of a matrix A of type (B) is determined in (5.3) as

$$\mathscr{C}(A) = \left\{ \begin{bmatrix} a & & \\ & e & f \\ & h & i \end{bmatrix} : a, e, f, h, i \in GF(p) \right\}.$$

We will determine the number of neighbors for each type separately.

(A) Obviously, the subring of scalar matrices is inside the centralizer, so the unique vertex of type (A) is in the neighborhood of vertex v, i.e. $N(A,B) = 1$.

Table 6.1: Neighborhood of a vertex v of type (A).

	(A)
(A)	1
(B)	$(p^2+p+1)p^2$
(C)	$\frac{1}{6}(p^2+p+1)p^3(p+1)$
(D)	$(p^3-1)(p+1)$
(E)	$(p^2+p+1)(p+1)$
(F)	$(p^2+p+1)p^2(p+1)$
(G)	$\frac{1}{3}(p^3-p)(p^3-p^2)$
(H)	$\frac{1}{2}(p^3-1)p^3$

(B) Let B be an arbitrary matrix from the centralizer such that B is of type (B), i.e.,

$$B = \begin{bmatrix} a & & \\ & e & f \\ & h & i \end{bmatrix} \text{ similar to } \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \beta \end{bmatrix}.$$

where α and β, $\beta \neq \alpha$, are from $GF(p)$. This will happen in two subcases

1) Suppose $\left[\begin{smallmatrix} e & f \\ h & i \end{smallmatrix}\right]$ is similar to a scalar matrix, i.e. if it is a scalar matrix, as there are no matrices similar to scalar out of themselves. This is equivalent to

$$\begin{cases} e = \beta, \\ f = 0, \\ h = 0, \\ i = \beta, \\ a = \alpha. \end{cases}$$

This implies that for α we have p possibilities, for β one option less, i.e., $p-1$. For a chosen eigenvalues we have exactly one matrix of type (B) inside of centralizer $\mathscr{C}(A)$. So, in total we have $p(p-1) \cdot 1 = p(p-1)$ matrices of type (B) in this subcase.

2) If $\left[\begin{smallmatrix} e & f \\ h & i \end{smallmatrix}\right]$ is a non-scalar, then, in order that B is similar to $\left[\begin{smallmatrix} \alpha & & \\ & \beta & \\ & & \beta \end{smallmatrix}\right]$, matrix $\left[\begin{smallmatrix} e & f \\ h & i \end{smallmatrix}\right]$ has to be diagonalizable with two different eigenvalues α and β, and a is either α or β. From Table 4.1 we know that the number of diagonalisable 2×2 matrices with two different eigenvalues, i.e., 2×2 matrices of type (B), is $\frac{(p+1)p}{2} \cdot p(p-1)$, the number of vertices times the number of matrices compressed into one vertex. For any such matrix we have 2 options for a. So, we have $(p+1)p \cdot p(p-1) = p^2(p+1)(p-1)$ matrices of type (B) in this subcase.

In total, we have $p(p-1) + p^2(p+1)(p-1) = p(p-1)(p^2+p+1)$ matrices of type (B) inside the centralizer $\mathscr{C}(A)$.

If one matrix is in the centralizer, the whole subring generated by that matrix is in the centralizer, so we divide the previously calculated number of matrices by the number of generators of a subring of type (B), see second column of Table 5.1, to get the number of vertices of type (B) which are in the neighborhood of vertex v, i.e.,

$$N(B,B) = \frac{p(p-1)(p^2+p+1)}{p(p-1)} = p^2+p+1.$$

(C) Let B be an arbitrary matrix from the centralizer $\mathscr{C}(A)$ such that B is of type (C) i.e.,

$$B = \begin{bmatrix} a & & \\ & e & f \\ & h & i \end{bmatrix} \text{ is similar to } \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \nu \end{bmatrix},$$

where λ, μ and ν are three different eigenvalues from the field $GF(p)$. This will be the case if and only if $\left[\begin{smallmatrix} e & f \\ h & i \end{smallmatrix}\right]$ is diagonalisable with two different eigenvalues and $a \in GF(p)$ is different from previously mentioned eigenvalues. From Table 4.1 we know that the number of diagonalisable 2×2 matrices with two different eigenvalues, i.e., 2×2 matrices of type (B), is $\frac{(p+1)p}{2} \cdot p(p-1)$, the number of vertices of type (B) times the number of matrices compressed into one vertex. Furthermore, we have $p-2$ options for a, so in total we have $\frac{(p+1)p}{2} \cdot p(p-1) \cdot (p-2)$ such 3×3 matrices. Similarly as in case (B), if we divide this number by the number of generators of a subring of type (C), see second column of Table 5.1, we get the number of vertices of type (C) which are in the neighborhood of vertex v, i.e.,

$$N(C,B) = \frac{\frac{(p+1)p}{2} \cdot p(p-1)\cdot(p-2)}{p(p-1)(p-2)} = \frac{p^2+p}{2}.$$

(D) Note that all matrices of type (D) have only one linearly independent eigenvector. Since the matrices from the centralizer $\mathscr{C}(A)$ are block-diagonal, we see that all of them have at least two linearly independent eigenvectors in the algebraic closure of the field $GF(p)$, meaning that there are no matrices of type (D) inside the centralizer, i.e., $N(D,B) = 0$.

(E) From the Table 4.1 we know that the number of 2×2 matrices with one double eigenvalue and minimal polynomial of degree 2 is $(p+1)\cdot p(p-1)$, the number of vertices of type (C) times the number of matrices compressed into one vertex. So, the number of matrices of type (E) in the centralizer $\mathscr{C}(A)$ is $(p+1)p(p-1)\cdot 1 = (p+1)p(p-1)$ because in case (E) we have matrices with triple eigenvalue. Finally, we divide the number of matrices by the number of generators of a subring type (E), which is $p(p-1)$, to get the number of vertices of type (E) in the neighborhood of vertex v, i.e.,

$$N(E,B) = \frac{(p+1)p(p-1)}{p(p-1)} = p+1.$$

(F) Similarly as in the previous case, we know that the number of matrices of type (F) in the centralizer is $(p+1)p(p-1)\cdot(p-1)$ because now we have two different eigenvalues, and thus $p-1$ choices for a. After we divide by the number of generators of a subring of type (F), which is $p(p-1)^2$, we get the number of vertices of type (F) in the neighborhood of vertex v, i.e.,

$$N(F,B)=\frac{p(p-1)(p+1)(p-1)}{p(p-1)^2}=p+1.$$

(G) As all the matrices from the centralizer have at least one eigenvalue from the field $GF(p)$, there are no matrices of type (G) in the centralizer, so vertex v has no neighbors of type (G), i.e., $N(G,B)=0$.

(H) Let B be an arbitrary matrix from the centralizer $\mathscr{C}(A)$, i.e.,

$$B=\begin{bmatrix} a & & \\ & e & f \\ & h & i \end{bmatrix}.$$

Matrix B is of a type (H) if and only if the 2×2 block is one of the $\frac{1}{2}(p^2-p)\cdot(p^2-p)$ matrices with irreducible characteristic polynomial, see row (D) of the Table 4.1, and a is an arbitrary element from the field $GF(p)$. So, the number of matrices of type (H) inside the centralizer is $\frac{1}{2}(p^2-p)(p^2-p)\cdot p$. If we divide this number by the number of generators of a subring of type (H), which is $p^2(p-1)$, we get the number of vertices of type (H) in the neighborhood of vertex v, i.e.,

$$N(H,B)=\frac{\frac{1}{2}(p^2-p)(p^2-p)p}{p^2(p-1)}=\frac{p(p-1)}{2}.$$

The results of the above calculations are collected in Table 6.2.

Table 6.2: Neighborhood of a vertex v of type (B).

	(B)
(A)	1
(B)	p^2+p+1
(C)	$\frac{p^2+p}{2}$
(D)	0
(E)	$p+1$
(F)	$p+1$
(G)	0
(H)	$\frac{p(p-1)}{2}$

Case (C): The centralizer of a matrix A of type (C) is determined in (5.6) as

$$\mathscr{C}(A) = \langle A \rangle_1 = \left\{ \begin{bmatrix} a & & \\ & b & \\ & & c \end{bmatrix} : a, b, c \in GF(p) \right\}.$$

(A) While calculating the number of generators of subring type (C) in Chapter 5, we detected the conditions for a matrix from $\mathscr{C}(A) = \langle A \rangle_1$ to generate a subring of dimension 1 or 2, i.e., when the matrix represents a vertex of type (A) or (B). For the vertex of type (A) the condition was $a = b = c$ and since we have only one vertex of type (A) we have

$$N(A, C) = 1.$$

(B) For the vertex of type (B) the condition was $b = c \neq a$, $a = b \neq c$ or $a = c \neq b$. In each of the three subcases we get one subring and those three subrings are different, so in the neighborhood of the vertex v we have 3 vertices of type (B), i.e.,

$$N(B, C) = 3.$$

(C) According to Proposition 4.4 there is exactly one vertex of type (C) in the neighborhood of vertex v, namely v itself, i.e.,

$$N(C, C) = 1.$$

Since in the $\mathscr{C}(A) = \langle A \rangle_1$ all matrices are diagonal, there are no vertices of types (D), (E), (F), (G) and (H) in the neighborhood of vertex v, i.e.,

$$N(D, C) = N(E, C) = N(F, C) = N(G, C) = N(H, C) = 0.$$

The results of the above calculations are collected in Table 6.3.

Table 6.3: Neighborhood of a vertex v of type (C).

	(C)
(A)	1
(B)	3
(C)	1
(D)	0
(E)	0
(F)	0
(G)	0
(H)	0

Case (D): The centralizer of a matrix A of type (D) is determined in (5.11) and (5.10) as

$$\mathscr{C}(A)=\left\{\begin{bmatrix}a & b & c\\ & a & b\\ & & a\end{bmatrix} : a,b,c\in GF(p)\right\}.$$

All matrices from the centralizer have one triple eigenvalue from the field $GF(p)$, i.e., possible types inside centralizer are (A), (D) and (E) while all other types are not possible. This means that

$$N(B,D)=N(C,D)=N(F,D)=N(G,D)=N(H,D)=0.$$

(A) While calculating the number of generators of subring type (D) in Chapter 5, we detected the condition for a matrix from $\mathscr{C}(A)=\langle A\rangle_1$ to generate a subring of dimension 1, i.e., when the matrix represents a vertex of type (A). It was $b=0$ and $c=0$ and since we have only one vertex of type (A) we have

$$N(A,D)=1.$$

(D) According to the Proposition 4.4 there is exactly one vertex of type (D) in the neighborhood of vertex v, namely v itself, i.e.,

$$N(D,D)=1.$$

(E) For the subring of dimension 2 the condition was $b=0$ and $c\neq 0$. It means that out of p^3 matrices in the centralizer, we have $p\cdot 1\cdot(p-1)=p(p-1)$ matrices that individually generate a subring of dimension 2. As subring of type (E) has $p(p-1)$ generators, see Table 5.1, in the neighborhood of the vertex v we have $\frac{p(p-1)}{p(p-1)}=1$ vertex of type (E). So,

$$N(E,D)=1.$$

The results of the above calculations are collected in Table 6.4.

Case (E): The centralizer of a matrix A of type (E) is determined in (5.15) as

$$\mathscr{C}(A)=\left\{\begin{bmatrix}a & b & c\\ 0 & a & 0\\ 0 & h & i\end{bmatrix} : a,b,c,h,i\in GF(p)\right\}.$$

A matrix B from the centralizer has eigenvalues a,a and i from the field $GF(p)$, which means that cases (C), (G) and (H) are not possible, i.e.,

$$N(C,E)=N(G,E)=N(H,E)=0.$$

We consider two possibilities concerning the eigenvalues.

Table 6.4: Neighborhood of a vertex v of type (D).

	(D)
(A)	1
(B)	0
(C)	0
(D)	1
(E)	1
(F)	0
(G)	0
(H)	0

1) If $i = a$ we have a matrix $B = \left[\begin{smallmatrix} a & b & c \\ & a & \\ & h & a \end{smallmatrix}\right]$ with triple eigenvalue a from the field $GF(p)$. Now we look at the number of eigenvectors, in order to detect the types of matrices. We find eigenvectors for the eigenvalue a by solving the matrix equation $(B - aI) \cdot v = 0$, which is equivalent to

$$\begin{bmatrix} 0 & b & c \\ & 0 & \\ & h & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

It is further equivalent to the system

$$\begin{cases} by + cz = 0, \\ hy = 0. \end{cases} \tag{6.1}$$

Note that x is a free variable. We will break the system solving into cases and subcases, as follows.

(a) If $h = 0$ we have $B = \left[\begin{smallmatrix} a & b & c \\ & a & \\ & & a \end{smallmatrix}\right]$ and system (6.1) is equivalent to

$$by + cz = 0.$$

(i) If $b = 0$ and $c = 0$ then $B = \left[\begin{smallmatrix} a & & \\ & a & \\ & & a \end{smallmatrix}\right]$, i.e., B is a scalar matrix. We have p such matrices and they are of type (A).

(ii) If $b \neq 0$ and $c = 0$ then $B = \left[\begin{smallmatrix} a & b & \\ & a & \\ & & a \end{smallmatrix}\right]$ and system (6.1) is equivalent to

$$by = 0.$$

with solution $y = 0$. Now, we have that z is a free variable so we have two linearly independent eigenvectors. This means that B is of type (E). There are $p \cdot (p - 1)$ such a matrices.

(iii) If $b = 0$ and $c \neq 0$ then $B = \begin{bmatrix} a & & c \\ & a & \\ & & a \end{bmatrix}$ and system (6.1) is equivalent to

$$cz = 0 \Leftrightarrow z = 0.$$

Now, y is free variable so we have again two eigenvectors and matrix B is of type (E). There are $p \cdot 1 \cdot (p-1) \cdot 1 \cdot 1 = p(p-1)$ such a matrices.

(iv) If $b \neq 0$ and $c \neq 0$ then $B = \begin{bmatrix} a & b & c \\ & a & \\ & & a \end{bmatrix}$ and system (6.1) is equivalent to

$$z = -\frac{by}{c}.$$

Here, y is a free variable, as is x, so we have two linearly independent eigenvectors which means that matrix B is of type (E). There are $p \cdot (p-1) \cdot (p-1) = p(p-1)^2$ such a matrices.

(b) If $h \neq 0$ then $B = \begin{bmatrix} a & b & c \\ & a & \\ & h & a \end{bmatrix}$ and the system (6.1) is equivalent to

$$\begin{cases} by + cz = 0, \\ y = 0, \end{cases}$$

which is further equivalent to

$$\begin{cases} cz = 0, \\ y = 0. \end{cases}$$

We consider two possibilities with respect to the value of parameter c.

(i) If $c = 0$ then z is a free variable so we have two linearly independent two eigenvectors which means that matrix B is of type (E). There are $p \cdot p \cdot (p-1) = p^2(p-1)$ such matrices.

(ii) If $c \neq 0$ then $z = 0$ so we have only one linearly independent eigenvector so matrix B is of type (D). There are $p \cdot p \cdot (p-1) \cdot (p-1) = p^2(p-1)^2$ such matrices.

2) If $i \neq a$ we have a matrix $B = \begin{bmatrix} a & b & c \\ & a & \\ & h & i \end{bmatrix}$ with two different eigenvalues. Namely, a of the algebraic multiplicity 2 and i of the algebraic multiplicity 1. Once again, we will consider the number of eigenvectors in order to detect the types of matrices. Obviously, eigenvalue i will have one linearly independent eigenvector, as geometric multiplicity is no greater than the algebraic multiplicity.

For the eigenvectors with eigenvalue a we have matrix equation $(B - aI) \cdot v = 0$, which is equivalent to

$$\begin{bmatrix} 0 & b & c \\ & 0 & \\ & h & i-a \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

It is further equivalent to the system

$$\begin{cases} by + cz = 0, \\ hy + (i-a)z = 0. \end{cases} \tag{6.2}$$

Note that x is a free variable. Now we consider two possible cases.

(a) Eigenvalue a has only one linearly independent eigenvector. This is the case if and only if the system (6.2) has only the trivial solution, as it is homogeneous. This holds if and only if

$$\begin{vmatrix} b & c \\ h & i-a \end{vmatrix} \neq 0,$$

which is equivalent to $b \neq \frac{ch}{i-a}$. So, in this case matrix B has two linearly independent eigenvectors and is of type (F). The number of such matrices B is $p \cdot (p-1) \cdot p \cdot p \cdot (p-1) = p^3(p-1)^2$.

(b) Eigenvalue a has more than one linearly independent eigenvector. This happens if and only if $b = \frac{ch}{i-a}$. Then system (6.2) has non-trivial solutions. It is equivalent to

$$\begin{cases} \frac{ch}{i-a} y + cz = 0, \\ hy + (i-a)z = 0, \end{cases}$$

which is further equivalent to

$$\begin{cases} c(hy + (i-a)z) = 0, \\ hy + (i-a)z = 0. \end{cases}$$

The last system is equivalent to $z = -\frac{hy}{i-a}$ and y is free variable. So eigenvalue a has exactly two linearly independent eigenvectors, i.e., matrix B has three linearly independent eigenvectors which means that it is of type (B). There are $p \cdot p \cdot p \cdot (p-1) = p^3(p-1)$ matrices in this subcase.

Recapitulating the previous calculation, we detected matrices of type (A) only in the subcase 1)-(a)-(i). As there is only one vertex of type (A) we have

$$N(A, E) = 1.$$

Matrices of type (B) were detected only in subcase 2)-(b), the number of matrices was $p^3(p-1)$. If we divide this number by the number of generators in case (B) we get

$$N(B, E) = \frac{p^3(p-1)}{p(p-1)} = p^2.$$

In subcase 1)-(b)-(ii) we detected matrices of type (D) and it was the only case with matrices of this type. The number of matrices was $p^2(p-1)^2$ and if we divide this number by the number of generators in case (D), we get

$$N(D,E) = \frac{p^2(p-1)^2}{p^2(p-1)} = p-1.$$

Matrices of type (E) were detected in numerous subcases, namely in 1)-(a)-(ii), 1)-(a)-(iii), 1)-(a)-(iv) and 1)-(b)-(i). We obtain the total number of matrices of type (E) by summing the numbers of matrices from the subcases. We get

$$p(p-1)+p(p-1)+p(p-1)^2+p^2(p-1) = p(p-1)(1+1+p-1+p) = p(p-1)(2p+1).$$

If we divide this number by the number of generators in case (E), we get

$$N(E,E) = \frac{p(p-1)(2p+1)}{p(p-1)} = 2p+1.$$

In the remaining subcase (2)-(a) we detected matrices of type (F), namely the number of matrices was $p^3(p-1)$ and if we divide it by the number of generators of type (F) we get

$$N(F,E) = \frac{p^3(p-1)^2}{p(p-1)^2} = p^2.$$

The results of the above calculations are collected in Table 6.5.

Table 6.5: Neighborhood of a vertex v of type (E).

	(E)
(A)	1
(B)	p^2
(C)	0
(D)	$p-1$
(E)	$2p+1$
(F)	p^2
(G)	0
(H)	0

Case (F): The centralizer of a matrix A of type (F) is determined in (5.19) and (5.18) as

$$\mathscr{C}(A) = \left\{ \begin{bmatrix} a & c & \\ & a & \\ & & b \end{bmatrix} : a,b,c \in GF(p) \right\}.$$

Let B be an arbitrary matrix from the centralizer. We consider four possibilities.

1. If $b = a$ and $c = 0$ then matrix is of type (A). There is unique subring of type (A), so vertex v has one neighbor of type (A), i.e.,
$$N(A, F) = 1.$$

2. If $b = a$ and $c \neq 0$ then matrix B is of type (E), because $\deg m_B = \dim_{GF(p)} \langle B \rangle_1 = 2$. The number of matrices of type (E) inside the centralizer is $p \cdot 1 \cdot (p-1)$. As a subring of type (E) has $p(p-1)$ generators we conclude that vertex v of type (F) has $\frac{p(p-1)}{p(p-1)} = 1$ neighbor of type (E), i.e.,
$$N(E, F) = 1.$$

3. If $b \neq a$ and $c = 0$ then matrix B generates a subring of type (B). The number of matrices of type (B) inside the centralizer is $p \cdot (p-1) \cdot 1 = p(p-1)$. As a subring of type (B) has $p(p-1)$ generators, we conclude that vertex v of type (F) has $\frac{p(p-1)}{p(p-1)} = 1$ neighbor of type (B), i.e.,
$$N(B, F) = 1.$$

4. If $b \neq a$ and $c \neq 0$ then matrix B has two different eigenvalues and $m_B = (x-a)^2(x-b)$ because $c \neq 0$, i.e., B is of type (F). The number of matrices of type (F) inside the centralizer is $p \cdot (p-1) \cdot (p-1) = p(p-1)^2$. As a subring of type (F) has $p(p-1)^2$ generators, we conclude that vertex v of type (F) has $\frac{p(p-1)^2}{p(p-1)^2} = 1$ neighbor of type (F), i.e.,
$$N(F, F) = 1.$$

   The same can be concluded from Proposition 4.4.

All the other types are not present in the centralizer so
$$N(C, F) = N(D, F) = N(G, F) = N(H, F) = 0.$$

The results of the above calculations are collected in Table 6.6.

Case (G): The centralizer of a matrix A of type (G) is determined in (5.25) and (5.27) as
$$\mathscr{C}(A) \cong GF(p^3).$$

In Chapter 5 we found out that the only subfield of the centralizer $\mathscr{C}(A) \cong GF(p^3)$, and hence the only subring, is isomorphic to $GF(p)$. This means that the vertex v of type (G) has only two neighbors: unique vertex of type (A) and v itself, i.e.,
$$N(A, G) = N(G, G) = 1$$

and
$$N(B, G) = N(C, G) = N(D, G) = N(E, G) = N(F, G) = N(H, G) = 0.$$

Table 6.6: Neighborhood of a vertex v of type (F).

	(F)
(A)	1
(B)	1
(C)	0
(D)	0
(E)	1
(F)	1
(G)	0
(H)	0

Table 6.7: Neighborhood of a vertex v of type (G).

	(G)
(A)	1
(B)	0
(C)	0
(D)	0
(E)	0
(F)	0
(G)	1
(H)	0

These results are collected in Table 6.7.

Case (H): The centralizer of a matrix A of type (H) is determined in (5.38) and (5.37) as the set of matrices of the form

$$B = \left[\begin{array}{c|cc} a & & \\ \hline & b & -ca_0 \\ & c & b - ca_1 \end{array}\right]$$

where $a, b, c \in GF(p)$ are arbitrary and a_1 and a_0 are fixed and depend on A. In Chapter 5, Case (H), we showed that matrix B is a generator of the subring $\langle A \rangle_1$, i.e., it is of type (H), if and only if $c \neq 0$. This means that there are $p \cdot p \cdot (p-1) = p^2(p-1)$ matrices of type (H) inside the centralizer. Dividing by the number of generators of a subring of type (H) we obtain

$$N(H, H) = \frac{p^2(p-1)}{p^2(p-1)} = 1.$$

For $c = 0$ we have $B = \begin{bmatrix} a & & \\ & b & \\ & & b \end{bmatrix}$. If $b = a$ then matrix B is a scalar matrix, so vertex v has a unique neighbor of type (A), i.e.,

$$N(A, H) = 1.$$

If $b \neq a$ matrix B is of type (B). We have $p \cdot (p-1)$ such matrices, and if we divide it by the number of generators of a subring of type (B) we get

$$N(B, H) = \frac{p(p-1)}{p(p-1)} = 1.$$

The results of the above calculations are collected in Table 6.8.

Table 6.8: Neighborhood of a vertex v of type (H).

	(H)
(A)	1
(B)	1
(C)	0
(D)	0
(E)	0
(F)	0
(G)	0
(H)	1

The results about the neighborhoods of all the vertices of the $\Lambda_1(\mathcal{M}_3(GF(p)))$ obtained in this chapter are summarized in Table 6.9.

Table 6.9: Neighborhoods of vertices of $\Lambda_1(\mathcal{M}_3(GF(p)))$.

	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)
(A)	1	1	1	1	1	1	1	1
(B)	$(p^2+p+1)p^2$	p^2+p+1	3	0	p^2	1	0	1
(C)	$\frac{1}{6}(p^2+p+1)p^3(p+1)$	$\frac{1}{2}(p^2+p)$	1	0	0	0	0	0
(D)	$(p^3-1)(p+1)$	0	0	1	$p-1$	0	0	0
(E)	$(p^2+p+1)(p+1)$	$p+1$	0	1	$2p+1$	1	0	0
(F)	$(p^2+p+1)p^2(p+1)$	$p+1$	0	0	p^2	1	0	0
(G)	$\frac{1}{3}(p^3-p)(p^3-p^2)$	0	0	0	0	0	1	0
(H)	$\frac{1}{2}(p^3-1)p^3$	$\frac{1}{2}p(p-1)$	0	0	0	0	0	1

Chapter 7

Subgraph induced on $V_{(B)} \cup V_{(E)}$

In this chapter we are going to describe the subgraph of the $\Lambda^1(\mathcal{M}_3(GF(p)))$ induced on the set $V_{(B)} \cup V_{(E)}$. We will refer to this subgraph as (B)-(E) graph. In order to describe (B)-(E) graph, we are going to use projective plane over the field $GF(p)$. The motivation for this approach is as follows. Take a vertex v of type (B) and suppose it is represented by a matrix A. We know that matrix A is diagonalisable, with two different eigenvalues in $GF(p)$. Without lost of generality we can assume that A is diagonal with eigenvalues λ and μ, i.e.,

$$A = \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix}.$$

Note that vertex v is also represented by matrix $A - \mu I$, which induces a decomposition of the vector space $GF(p)^3$ in the sense that

$$GF(p)^3 = \operatorname{Im}(A - \mu I) \oplus \operatorname{Ker}(A - \mu I) \cong GF(p) \oplus GF(p)^2.$$

As 1-dimensional subspace $\operatorname{Im}(A - \mu I)$ represents a point P in a projective plane and 2-dimensional subspace $\operatorname{Ker}(A - \mu I)$ represents a line L, it is natural to use projective plane to describe vertices of type (B). Once P and L are given, a diagonal matrix A is uniquely determined up to the eigenvalues λ and μ, as we will show in Section 7.2. Similar consideration can be done also for a vertex of type (E).

7.1 Projective plane over $GF(p)$ and its incidence matrix

Let us recall the notion of the projective plane over the field $GF(p)$, which we denote by $PG(2, p)$, see [11]. Consider the set of all 1-dimensional subspaces of the vector space $GF(p)^3$ and denote it by $\mathscr{P}$ and the set of all 2-dimensional subspaces of the vector space $GF(p)^3$ and denote it by $\mathscr{L}$. The points of the projective plane $PG(2, p)$ are the elements of $\mathscr{P}$ while the lines are the elements of $\mathscr{L}$. Furthermore, a point $P \in \mathscr{P}$ lies on a line $L \in \mathscr{L}$ if and only if $P \subset L$ and we denote this by $P \in L$.

The cardinality of the set of points $\mathscr{P}$ is given as the Gaussian p-binomial coefficient with $n = 3$ and $k = 1$, i.e.

$$|\mathscr{P}| = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_p = \frac{p^3 - 1}{p - 1} = p^2 + p + 1.$$

The cardinality of the set of lines $\mathscr{L}$ is equal to

$$|\mathscr{L}| = \begin{bmatrix} 3 \\ 2 \end{bmatrix}_p = \frac{(p^3 - 1)(p^2 - 1)}{(p^2 - 1)(p - 1)} = p^2 + p + 1.$$

Every line contains

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p = \frac{p^2 - 1}{p - 1} = p + 1$$

points and every point P lies on

$$\begin{bmatrix} 2 \\ 1 \end{bmatrix}_p = p + 1$$

lines, because 2-dimensional subspaces of $GF(p)^3$ that contain 1-dimensional subspace P are in a bijective correspondence with 1-dimensional subspaces of the 2-dimensional factor space $GF(p)^3/P$. The plane $PG(2, p)$ can be described by incidence matrix which is 0-1 matrix of the order $(p^2 + p + 1) \times (p^2 + p + 1)$. Each row of the incidence matrix corresponds to a point and each column of the matrix corresponds to a line, where (P, L) entry of the matrix is 1 if $P \in L$, otherwise it is 0. Each row and each column of incidence matrix contains exactly $p + 1$ ones.

We denote

$$\mathscr{B} = \{(P, L) \in \mathscr{P} \times \mathscr{L} : P \notin L\} \tag{7.1}$$

and

$$\mathscr{E} = \{(P, L) \in \mathscr{P} \times \mathscr{L} : P \in L\}. \tag{7.2}$$

Elements of $\mathscr{B}$ correspond to zeros in the incidence matrix and elements of $\mathscr{E}$ correspond to ones. Obviously, $|\mathscr{E}| = (p + 1)(p^2 + p + 1)$ and $|\mathscr{B}| = p^2(p^2 + p + 1)$.

We will now explicitly describe the incidence matrix of the projective plane $PG(2, p)$. The description is adapted from [10]. Let e be the vector of length p with 1 at all positions, i.e.,

$$e = \begin{bmatrix} 1 & 1 & \cdots & 1 \end{bmatrix}^T \in \mathbb{R}^p.$$

For every $s \in \{1, 2, \ldots, p\}$ let $R_s \in \mathcal{M}_p(\mathbb{R})$ be the matrix with s-th row equal to e^T and all other entries 0, i.e.,

$$(R_s)_{i,j} = \begin{cases} 1, & \text{if } i = s, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, for every $s \in \{2, \ldots, p\}$ and every $t \in \{1, 2, \ldots, p\}$ let $S_{s,t} \in \mathcal{M}_p(\mathbb{R})$ be the permutation matrix defined as

$$\left(S_{s,t}\right)_{i,j} = \begin{cases} 1, & \text{if } (s-1)(i+j) \equiv t \pmod{p}, \\ 0, & \text{otherwise.} \end{cases}$$

Now, let $T_p \in \mathcal{M}_{1+p+p^2}(\mathbb{R})$ be 0-1 matrix defined as a block matrix

$$T_p = \begin{bmatrix} 1 & e^T & 0 & 0 & \cdots & 0 \\ e & 0 & R_1 & R_2 & \cdots & R_p \\ 0 & R_1^T & I_p & I_p & \cdots & I_p \\ 0 & R_2^T & S_{2,1} & S_{2,2} & \cdots & S_{2,p} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & R_p^T & S_{p,1} & S_{p,2} & \cdots & S_{p,p} \end{bmatrix}, \tag{7.3}$$

where I_p is the identity matrix order p. It is proved in the [10] that T_p is the incidence matrix of the plane $PG(2,p)$.

In the case $p = 2$ the incidence matrix T_2 of the projective plane $PG(2,2)$ (called also Fano plane) is

$$T_2 = \left[\begin{array}{c|cc|cc|cc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right].$$

In the case $p = 3$ the incidence matrix T_3 of the projective plane $PG(2,3)$ is

$$T_3 = \left[\begin{array}{c|ccc|ccc|ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

7.2 Bijection between $V_{(B)} \cup V_{(E)}$ and $\mathscr{P} \times \mathscr{L}$

We will now establish a bijection between the sets $V_{(B)}$ and $\mathscr{B}$. Let $v \in V_{(B)}$ be an arbitrary vertex. Let A be a matrix representative of the vertex v. Then there exists an invertible matrix S and $\lambda, \mu \in GF(p)$, $\mu \neq \lambda$, such that

$$A = S \begin{bmatrix} \lambda & & \\ & \mu & \\ & & \mu \end{bmatrix} S^{-1}.$$

Now we can define a mapping $\Phi_B : V_{(B)} \to \mathscr{B}$ by

$$\Phi_B(v) = (\mathrm{Im}(A - \mu I), \mathrm{Ker}(A - \mu I)). \tag{7.4}$$

Note that $L = \mathrm{Ker}(A - \mu I)$ is a 2-dimensional subspace of $GF(p)^3$ so it belongs to $\mathscr{L}$ and consequently $P = \mathrm{Im}(A - \mu I)$ is a 1-dimensional subspace of $GF(p)^3$ so it belongs to $\mathscr{P}$. Furthermore, the intersection of P and L is trivial subspace so $P \notin L$ which means that $\Phi_B(v)$ belongs to $\mathscr{B}$.

We need to prove that Φ_B is well defined, i.e., $\Phi_B(v)$ does not depend on the choice of the representative A. Suppose that B is another matrix representative of the vertex v. Then $\langle B \rangle_1 = \langle A \rangle_1 = \mathrm{Lin}\{I, A\}$ so $B = aI + bA$ where $b \neq 0$. It follows that

$$B = S \begin{bmatrix} a + b\lambda & & \\ & a + b\mu & \\ & & a + b\mu \end{bmatrix} S^{-1}.$$

Now we have

$$B - (a + b\mu)I = S \begin{bmatrix} b(\lambda - \mu) & & \\ & 0 & \\ & & 0 \end{bmatrix} S^{-1} = b(A - \mu I).$$

It follows that $\mathrm{Im}(B - (a + b\mu)I) = \mathrm{Im}(A - \mu I)$ and $\mathrm{Ker}(B - (a + b\mu)I) = \mathrm{Ker}(A - \mu I)$ which shows that $\Phi_B(v)$ is well defined.

Now, we want to show that mapping Φ_B is a bijection. In order to do that we define a mapping $\Psi_B : \mathscr{B} \to V_{(B)}$ as follows. Let $(P, L) \in \mathscr{B}$ be arbitrary. Let $\{b_1\}$ be the basis of P and $\{b_2, b_3\}$ be the basis of L. Since $P \notin L$ vectors b_1, b_2 and b_3 are linearly independent so the matrix $S = \begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix}$, with columns b_1, b_2 and b_3, is invertible. Take $\Psi_B(P, L)$ to be the vertex v in $V_{(B)}$ represented by the matrix of the idempotent linear operator with image P and kernel L, i.e., the matrix $A = SE_{1,1}S^{-1}$. Note that matrix A is independent of the choice of the basis vectors b_1, b_2 and b_3.

Since the matrix A has a double eigenvalue 0 and a simple eigenvalue 1, it is clear from the definition of Φ_B that $\Phi_B(v) = (\mathrm{Im}\, A, \mathrm{Ker}\, A) = (P, L)$, so that $\Phi_B \circ \Psi_B = \mathrm{Id}_{\mathscr{B}}$. Since $|V_{(B)}| = |\mathscr{B}| = p^2(p^2 + p + 1)$, we conclude that Φ is a bijection.

We will now establish a bijection between the sets $V_{(E)}$ and $\mathscr{E}$. Let $v \in V_{(E)}$ be an arbitrary vertex. Let A be a matrix representative of the vertex v. Then there exists an invertible matrix S and $\lambda \in GF(p)$, such that

$$A = S \begin{bmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{bmatrix} S^{-1}.$$

Now we can define a mapping $\Phi_E : V_{(E)} \to \mathscr{E}$ by

$$\Phi_E(v) = (\operatorname{Im}(A - \lambda I), \operatorname{Ker}(A - \lambda I)). \tag{7.5}$$

Note that $L = \operatorname{Ker}(A - \mu I)$ is a 2-dimensional subspace of $GF(p)^3$ so it belongs to $\mathscr{L}$ and $P = \operatorname{Im}(A - \mu I)$ is a 1-dimensional subspace of $GF(p)^3$ so it belongs to $\mathscr{P}$. Furthermore, $P \in L$ which means that $\Phi_E(v)$ belongs to $\mathscr{E}$.

We need to prove that Φ_E is well defined, i.e., $\Phi_E(v)$ does not depend on the choice of the representative A. Suppose that B is another matrix representative of the vertex v. Then $\langle B \rangle_1 = \langle A \rangle_1 = \operatorname{Lin}\{I, A\}$ so $B = aI + bA$ where $b \neq 0$. It follows that

$$B = S \begin{bmatrix} a + b\lambda & b & \\ & a + b\lambda & \\ & & a + b\lambda \end{bmatrix} S^{-1}.$$

Now we have

$$B - (a + b\lambda)I = S \begin{bmatrix} 0 & b & \\ & 0 & \\ & & 0 \end{bmatrix} S^{-1} = b(A - \lambda I).$$

It follows that $\operatorname{Im}(B - (a + b\lambda)I) = \operatorname{Im}(A - \lambda I)$ and $\operatorname{Ker}(B - (a + b\lambda)I) = \operatorname{Ker}(A - \lambda I)$ which shows that $\Phi_E(v)$ is well defined.

Now, we want to show that mapping Φ_E is a bijection. In order to do that we define a mapping $\Psi_E : \mathscr{E} \to V_{(E)}$ as follows. Let $(P, L) \in \mathscr{E}$ be arbitrary. Let $\{b_1\}$ be the basis of P and b_3 be the vector such that $\{b_1, b_3\}$ is basis of L. As a final step, let b_2 be the vector such that $\{b_1, b_2, b_3\}$ is basis of $GF(p)^3$. Now, we define matrix $S = \begin{bmatrix} b_1 & b_2 & b_3 \end{bmatrix}$, with columns b_1, b_2 and b_3, obviously invertible. Take $\Psi_E(P, L)$ to be the vertex v in $V_{(E)}$ represented by the matrix of the nilpotent linear operator with image P and kernel L, i.e., the matrix $A = SE_{1,2}S^{-1}$. Note that vertex v is independent of the choice of the vectors b_1, b_2 and b_3.

Since the matrix A has a triple eigenvalue 0, it is clear from the definition of Φ_E that $\Phi_E(v) = (\operatorname{Im} A, \operatorname{Ker} A) = (P, L)$, so that $\Phi_E \circ \Psi_E = \operatorname{Id}_{\mathscr{E}}$. Since $|V_{(E)}| = |\mathscr{E}| = (p^2 + p + 1)(p + 1)$, we conclude that Φ_E is a bijection.

We now combine the mappings Φ_B and Φ_E into a bijection

$$\Phi : V_{(B)} \cup V_{(E)} \to \mathscr{B} \cup \mathscr{E} = \mathscr{P} \times \mathscr{L}$$

defined by $\Phi|_{V_{(B)}} = \Phi_B$ and $\Phi|_{V_{(E)}} = \Phi_E$. Since $V_{(B)}$ and $V_{(E)}$ are disjoint, Φ is well defined. Since also $\mathscr{B}$ and $\mathscr{E}$ are disjoint and Φ_B and Φ_E are bijections, Φ is a bijection.

7.3 Geometrical interpretation of edges

We define a graph Δ with vertex set $V(\Delta) = \mathscr{P} \times \mathscr{L}$ and edges defined as follows. Let v_1 and v_2 be elements of $V_{(B)} \cup V_{(E)}$. There is an edge between $\Phi(v_1)$ and $\Phi(v_2)$ in Δ if and only if there is an edge between v_1 and v_2 in the compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$. This makes the mapping Φ into a graph isomorphism between the induced subgraph of $\Lambda^1(\mathcal{M}_3(GF(p)))$ on the set $V_{(B)} \cup V_{(E)}$ and Δ. Next theorem describes the edges of the graph Δ in geometric terms.

Theorem 7.1. *Let $(P_1, L_1), (P_2, L_2) \in \mathscr{P} \times \mathscr{L}$ be arbitrary. There is an edge between (P_1, L_1) and (P_2, L_2) in Δ if and only if one of the following conditions holds*

(a) $P_1 = P_2$ *and* $L_1 = L_2$,

(b) $P_1 \in L_1$, $P_2 \in L_2$, *and either* $P_1 = P_2$ *or* $L_1 = L_2$,

(c) $P_1 \neq P_2$, $L_1 \neq L_2$ *and* $P_2 \in L_1 \cap L_2$ *and* $P_1 \in L_2 \setminus L_1$,

(d) $P_1 \neq P_2$, $L_1 \neq L_2$ *and* $P_1 \in L_1 \cap L_2$ *and* $P_2 \in L_1 \setminus L_2$,

(e) $P_1 \neq P_2$, $L_1 \neq L_2$ *and* $P_1 \in L_2 \setminus L_1$ *and* $P_2 \in L_1 \setminus L_2$.

Proof. Let $(P_1, L_1) = \Phi(v_1)$ and $(P_2, L_2) = \Phi(v_2)$. Let A_1 be the matrix representative of v_1 with image P_1 and kernel L_1, and A_2 be the matrix representative of v_2 with image P_2 and kernel L_2.

($\Leftarrow$): Suppose that one of the conditions (a)–(e) holds.

(a) As $(P_1, L_1) = (P_2, L_2)$ and Φ is bijection then $v_1 = v_2$. Since every vertex in $\Lambda^1(\mathcal{M}_3(GF(p)))$ has a loop there is an edge between (P_1, L_1) and (P_2, L_2).

(b) The conditions imply that $(P_1, L_1), (P_2, L_2) \in \mathscr{E}$, so that $v_1, v_2 \in V_{(E)}$.

If $P_1 = P_2$ then $P_2 \in L_1$ and $P_1 \in L_2$, so $A_1A_2 = 0$ and $A_2A_1 = 0$. Combining last two equation we get $A_1A_2 = A_2A_1$ which means that there is an edge between v_1 and v_2, hence also between (P_1, L_1) and (P_2, L_2).

If $L_1 = L_2$ then again $P_2 \in L_1$ and $P_1 \in L_2$, and we obtain the same conclusion.

(c)–(e) Each set of the conditions imply that $P_2 \in L_1$ and $P_1 \in L_2$, so there is an edge between (P_1, L_1) and (P_2, L_2), as shown above.

($\Rightarrow$): Suppose that there is an edge between (P_1, L_1) and (P_2, L_2) in Δ. Then there is an edge between v_1 and v_2 so we have $A_1A_2 = A_2A_1$. If $(P_1, L_1) = (P_2, L_2)$ then condition (a) holds. So suppose that $(P_1, L_1) \neq (P_2, L_2)$. Note that matrices A_1 and A_2 are of rank 1, as their images are P_1 and P_2, which are vector subspaces of dimension 1.

We claim that $A_1A_2 = 0$. Suppose this is not the case. Then $\operatorname{rank}(A_1A_2) = 1$. This implies that $\operatorname{Im}(A_1A_2) = \operatorname{Im}(A_1) = P_1$ and $\operatorname{Ker}(A_1A_2) = \operatorname{Ker}(A_2) = L_2$. As $A_1A_2 = A_2A_1$, we conclude similarly $\mathrm{Im}(A_2A_1) = \mathrm{Im}(A_2) = P_2$ and $\mathrm{Ker}(A_2A_1) = \mathrm{Ker}(A_1) = L_1$. Hence, $P_1 = P_2$ and $L_1 = L_2$ which is in contradiction with $(P_1, L_1) \neq (P_2, L_2)$. This proves our claim.

From the above we get $A_1A_2 = 0$ and $A_2A_1 = 0$. This implies $P_2 \in L_1$ and $P_1 \in L_2$. We now consider four cases:

(*i*) $P_1 \in L_1$ and $P_2 \in L_2$: If $P_1 = P_2$ or $L_1 = L_2$ then the condition (b) holds. So, suppose the opposite $P_1 \neq P_2$ and $L_1 \neq L_2$. This means that two different points P_1 and P_2 lie at the same time on two different lines L_1 and L_2, which is impossible.

(*ii*) $P_1 \notin L_1$ and $P_2 \in L_2$: Since $P_1 \notin L_1$ and $P_2 \in L_1$ we have $P_1 \neq P_2$. Similarly, as $P_1 \notin L_1$ and $P_1 \in L_2$ we get $L_1 \neq L_2$. Furthermore, $P_2 \in L_1 \cap L_2$ and $P_1 \in L_2 \setminus L_1$. Hence, condition (c) holds.

(*iii*) $P_1 \in L_1$ and $P_2 \notin L_2$: Since $P_2 \notin L_2$ and $P_1 \in L_2$ we have $P_1 \neq P_2$. Similarly, as $P_2 \notin L_2$ and $P_2 \in L_1$ we get $L_1 \neq L_2$. Furthermore, $P_1 \in L_1 \cap L_2$ and $P_2 \in L_1 \setminus L_2$. Hence, condition (d) holds.

(*iv*) $P_1 \notin L_1$ and $P_2 \notin L_2$: Since $P_1 \in L_2$ and $P_1 \notin L_1$ we get $P_1 \in L_2 \setminus L_1$. Similarly, as $P_2 \in L_1$ and $P_2 \notin L_2$ we get $P_2 \in L_1 \setminus L_2$. This implies that $P_1 \neq P_2$ and $L_1 \neq L_2$, hence condition (e) holds.

This finishes the proof. □

We remark that condition (a) of Theorem 7.1 describes the loops in Δ. Condition (b) describes the edges between two different vertices in $\mathscr{E}$, it means that two ones in the incidence matrix are connected if and only if they lie in the same row or in the same column. Conditions (c) and (d) describe edges between vertices in $\mathscr{B}$ and $\mathscr{E}$, it means that 0 and 1 in incidence matrix are connected if and only if they lie in different rows and columns, and the other two entries of the 2×2 submatrix of T_p, which contains the two entries 0 and 1, are both equal to 1. Condition (e) describes edges between two different vertices in $\mathscr{B}$. It means that two zeros in incidence matrix T_p are connected if and only if they lie in different rows and columns, and the other two entries of the 2×2 submatrix of T_p, which contains the two zeros, are both equal to 1.

Figure 7.1 shows all possible 2×2 submatrices of T_p and the edges between their entries. The red vertices in the Figure are vertices of type (B) and correspond to the zeroes in matrix T_p, while the blue vertices are vertices of type (E) and correspond to ones in the matrix T_p. Note that 2×2 submatrix of T_p cannot contain only ones because that would mean that two different lines intersect two different points, which is not possible in the plane.

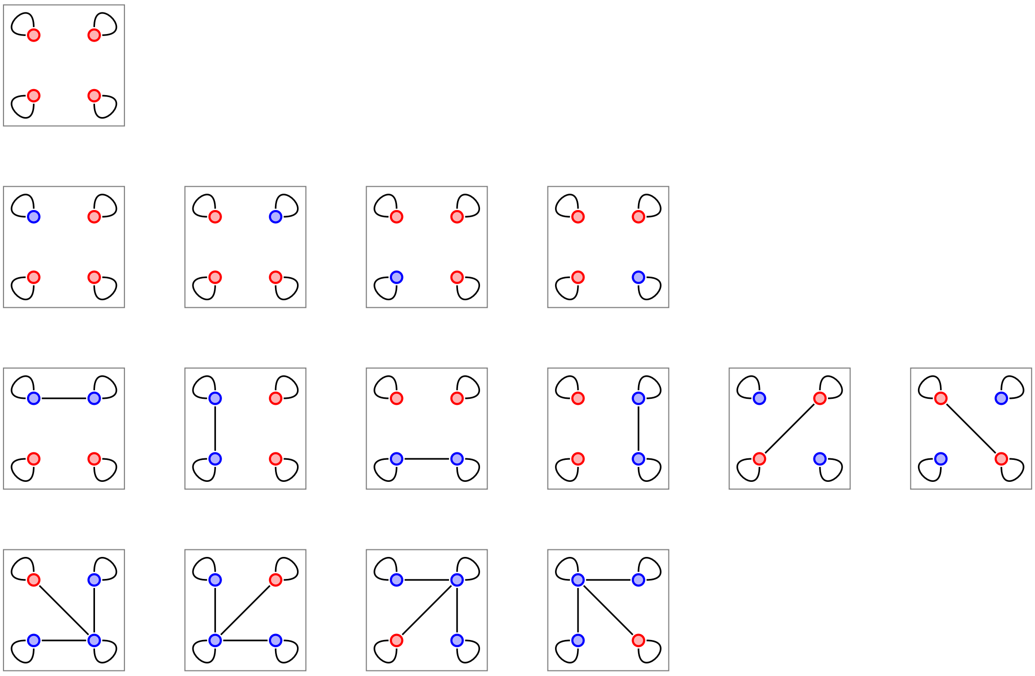

Figure 7.1: Possible 2 × 2 submatrices of T_p and the edges between their entries.

Chapter 8

Description of $\Lambda^1(\mathcal{M}_3(GF(p)))$

For convenience we recall Table 5.1 and Table 6.9. Table 8.1 gives the number of vertices of each type and the number of matrices compressed into each vertex. In Table 8.2 entry in the row (X) and column (Y) gives the number of vertices of type (X) in the neighborhood of a vertex of type (Y), so the column (Y) of the Table 8.2 corresponds to the neighborhood of the vertex of type (Y).

Table 8.1: Vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$.

CASE	Number of vertices	Number of matrices compressed	$\dim\langle A\rangle_1$
(A)	1	p	1
(B)	$(p^2+p+1)p^2$	$p(p-1)$	2
(C)	$\frac{1}{6}(p^2+p+1)p^3(p+1)$	$p(p-1)(p-2)$	3
(D)	$(p^3-1)(p+1)$	$p^2(p-1)$	3
(E)	$(p^2+p+1)(p+1)$	$p(p-1)$	2
(F)	$(p^2+p+1)p^2(p+1)$	$p(p-1)^2$	3
(G)	$\frac{1}{3}(p^3-p)(p^3-p^2)$	p^3-p	3
(H)	$\frac{1}{2}(p^3-1)p^3$	$p^2(p-1)$	3

8.1 Properties of $\Lambda^1(\mathcal{M}_3(GF(p)))$

Note that properties of (B)-(E) graph are described in Chapter 7. Here we describe the properties of the rest of the graph, according to the type of vertices. On the way we describe how to construct the graph $\Lambda^1(\mathcal{M}_3(GF(p)))$, starting with (B)-(E) graph and adding to it vertices of other type.

(C) Note that for $p=2$ there are no vertices of type (C). Suppose that $p\geq 3$. From the Table 8.1 we see that there are $\frac{1}{6}(p^2+p+1)p^3(p+1)$ vertices of type (C). From Table 8.2 we see

Table 8.2: Neighborhoods of vertices of $\Lambda^1(\mathcal{M}_3(GF(p)))$.

	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)
(A)	1	1	1	1	1	1	1	1
(B)	$(p^2+p+1)p^2$	p^2+p+1	3	0	p^2	1	0	1
(C)	$\frac{1}{6}(p^2+p+1)p^3(p+1)$	$\frac{1}{2}(p^2+p)$	1	0	0	0	0	0
(D)	$(p^3-1)(p+1)$	0	0	1	$p-1$	0	0	0
(E)	$(p^2+p+1)(p+1)$	$p+1$	0	1	$2p+1$	1	0	0
(F)	$(p^2+p+1)p^2(p+1)$	$p+1$	0	0	p^2	1	0	0
(G)	$\frac{1}{3}(p^3-p)(p^3-p^2)$	0	0	0	0	0	1	0
(H)	$\frac{1}{2}(p^3-1)p^3$	$\frac{1}{2}p(p-1)$	0	0	0	0	0	1

that there will be no (C)–(C) edges except the loop at on each vertex of type (C). Note that every vertex of type (C) is connected to precisely 3 vertices of type (B) and by (5.6) these 3 vertices form a triangle, because a subring generated by one matrix is automatically commutative. So, every vertex of type (C) is connected to the vertices of a unique triangle of (B) vertices in (B)-(E) graph. Now, we show the opposite, that to every triangle of (B) vertices correspond a (C) vertex, connected to them. Let $v_1 = [A_1]_1$, $v_2 = [A_2]_1$ and $v_3 = [A_3]_1$ be 3 different vertices of type (B) forming a triangle. Since matrices A_1, A_2 and A_3 are diagonalizable and they commute, they are simultaneously diagonalizable, i.e., there exists invertible matrix S such that $A_1 = SD_1S^{-1}$, $A_2 = SD_2S^{-1}$ and $A_3 = SD_3S^{-1}$. Take a set

$$\mathcal{D} = \{SDS^{-1} : D \text{ is diagonal }\}.$$

Obviously, $\mathcal{D}$ is a subring and it is an isomorphic copy of subring of all diagonal matrices, generated by any diagonal matrix with three different elements on the main diagonal. Generators of $\mathcal{D}$ are compressed into a vertex v of type (C). Since A_1, A_2 and A_3 are elements of $\mathcal{D}$, subrings $\langle A_1\rangle_1$, $\langle A_2\rangle_1$ and $\langle A_3\rangle_1$ are subrings of $\mathcal{D}$, i.e., v_1, v_2 and v_3 are connected to v. As a consequence, the number of triangles of vertices of type (B) is equal to the number of vertices of type (C), which is equal to $\frac{1}{6}(p^2+p+1)p^3(p+1)$.
So, to add vertices of type (C) to the existing graph, for every triangle of vertices of type (B) we add one vertex of type (C), connect it the vertices of the triangle and put a loop on the vertex of type (C).

(F) From the Table 8.1 we see that there are $(p^2+p+1)p^2(p+1)$ vertices of type (F). From Table 8.2 we see that there will be no (F)–(F) edges except a loop on each vertex of type (F). Note that every vertex of type (F) is connected to precisely one vertex of type (B) and one vertex of type (E). From (5.19) we see that those two vertices of type (B) and (E) are connected by an edge, because a subring generated by one matrix is automatically commutative. So, every vertex of type (F) is connected to the endpoints of a unique (B)–(E) edge. From Table 8.1 we know that the number of vertices of type (B) is $(p^2+p+1)p^2$

and from Table 8.2 we have that one vertex of type (B) is connected to $p+1$ vertices of type (E) so, we have in total $(p^2+p+1)p^2 \cdot (p+1)$ (B)–(E) edges. Note that we have the same number of vertices of type (F), hence, the endpoints of every (B)–(E) edge are connected to a unique vertex of type (F).
So, to add vertices of type (F) to the existing graph, for every (B)–(E) edge we add one vertex of type (F), connect it to the edge endpoints and put a loop on the vertex of type (F).

(H) From the Table 8.1 we see that there are $\frac{1}{2}(p^3-1)p^3$ vertices of type (H). From Table 8.2 we see that there will be no (H)–(H) edges except a loop at each vertex of type (H). Also, every vertex of type (G) will be connected to the unique vertex of type (A) and to one vertex of type (B). On the other hand, each vertex of type (B) has $\frac{p(p-1)}{2}$ vertices of type (H) in the neighborhood, see Table 8.2.
So, to add vertices of type (H) to the existing graph, we first partition the set of vertices of type (H) into $(p^2+p+1)p^2$ parts, each containing $\frac{p(p-1)}{2}$ vertices. Note that we have the same number of parts as the number of vertices of type (B). Now we put a loop on every vertex from one part, connect all vertices from this part to a fixed vertex of type (B). Then repeat the same procedure for the next part and vertex (B), until we spend all parts and vertices of type (B).

(D) From the Table 8.1 we see that there are $(p^3-1)(p+1)$ vertices of type (D). From Table 8.2 we see that there will be no (D)–(D) edges except a loop on each vertex of type (D) and that every vertex od type (D) will be connected to precisely one vertex of type (E) and to a unique vertex of type (A). On the other hand, from Table 8.2 we see that one vertex of type (E) has $p-1$ vertices of type (D) in the neighborhood.
So, to add vertices of type (D) to the existing graph, we first partition the set of vertices of type (D) into $(p^2+p+1)(p+1)$ parts, each containing $(p-1)$ vertices. Note that we have the same number of partitions as the number of vertices of type (E). Now we put a loop on every vertex from one part, connect all vertices from this part to a fixed vertex of type (E). Then repeat the same procedure for the next part and vertex (E), until we spend all parts and vertices of type (E).

(G) From the Table 8.1 we see that there are $\frac{1}{3}(p^3-p)(p^3-p^2)$ vertices of type (G). From Table 8.2 we see that there will be no (G)–(G) edges except a loop on each vertex of type (G) and that every vertex of type (G) is connected by an edge to the unique vertex of type (A), see Table 8.2.
So, we add $\frac{1}{3}(p^3-p)(p^3-p^2)$ vertices of type (G) to the existing graph and put a loop on every vertex of type (G).

(A) We add the unique vertex of type (A) and connect it to every other vertex and put a loop on it.

8.2 Construction of $\Lambda^1(\mathcal{M}_3(GF(p)))$

We construct the compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$ as follows:

1. We construct (B)-(E) graph described in Chapter 7. The vertices of type (B) correspond to the zeroes in the incidence matrix (7.3) of the projective geometry $PG(2,p)$ and the vertices of type (E) correspond to ones in the same matrix. The edges between these vertices are presented in the Figure 7.1.

2. If $p \geq 3$ then for every triangle of vertices of type (B) we add one vertex of type (C) and connect it the vertices of the triangle, otherwise omit this step.

3. For every (B)–(E) edge we add one vertex of type (F) and connect it to the edge endpoints.

4. For every vertex of type (B) we add $\frac{p(p-1)}{2}$ vertices of type (H) and connect them to the vertex of type (B).

5. For every vertex of type (E) we add $p-1$ vertices of type (D) and connect them to the vertex of type (E).

6. We add $\frac{1}{3}(p^3-p)(p^3-p^2)$ vertices of type (G).

7. We add one vertex of type (A) and connect it to every other vertex.

8. We put a loop on every vertex.

With this step, the construction of compressed commuting graph of the ring $\mathcal{M}_3(GF(p))$ is finished.

Chapter 9

Commuting graph of $\mathcal{M}_3(GF(p))$

In this chapter we demonstrate how compressed commuting graph can be used to describe the ordinary (non-compressed) commuting graph. For 2×2 matrices over a finite field $\mathbb{F}$ the structure of the commuting graph $\Gamma(\mathcal{M}_2(\mathbb{F}))$ is described in [2, Theorem 2]. In particular, this graph is a disjoint union of $|\mathbb{F}|^2 + |\mathbb{F}| + 1$ cliques of size $|\mathbb{F}|^2 - |\mathbb{F}|$. For 3×3 matrices the description of the commuting graph $\Gamma(\mathcal{M}_3(\mathbb{F}))$ is still an open problem. The graph was partially described in [22, Lemma 4.1] where the authors showed that the graph has only one connected component that is not a clique. Furthermore, every connected component that is a clique equals $\mathbb{F}[A] \setminus \mathbb{F}I$ where A is a non-derogatory matrix with irreducible minimal polynomial such that there is no intermediate field between fields $\mathbb{F}$ and $\mathbb{F}[A]$. Note that $\mathbb{F}[A]$ is a field as minimal polynomial is irreducible.

With the results of this thesis we can now completely describe the graph $\Gamma(\mathcal{M}_3(\mathbb{F}))$ in the case when $\mathbb{F} = GF(p)$. We will do this using the so-called "blow-up" process that was originally used for zero-divisor graphs in [16, 12].

We start with $\Lambda^1(\mathcal{M}_3(GF(p)))$ described in Chapter 8. To obtain the graph $\Gamma(\mathcal{M}_3(GF(p)))$ we first remove the unique vertex of type (A) and all edges incident to this vertex. Then, from every vertex we remove the loop. In the final step, we "blow-up" each vertex into several copies using the numbers from Table 8.1. In particular, for a vertex v of a certain type we can find in Table 8.1 the number of matrices that were compressed into vertex v, namely $|[A]_1|$, where A is a matrix representative of vertex v. We replace vertex v with a clique of size $|[A]_1|$ and connect every vertex of this clique to all other vertices that vertex v was connected to. Once we do this for all the vertices we obtain the graph $\Gamma(\mathcal{M}_3(GF(p)))$.

Note that after removing the unique vertex of type (A) along with all of his edges and all the loops from $\Lambda^1(\mathcal{M}_3(GF(p)))$, the graph breakes into several connected components. Some of these components are single vertices, and these are precisely vertices of type (G) and there are $\frac{1}{3}(p^3 - p)(p^3 - p^2)$ of them. After the "blow-up" process these become cliques of size $p^3 - p$ in $\Gamma(\mathcal{M}_3(GF(p)))$. There is only one additional connected component containing all the other vertices. This is in accordance with the partial description in [22, Lemma 4.1].

Bibliography

[1] S. Akbari, H. Bidkhori, and A. Mohammadian, *Commuting graphs of matrix algebras*, Comm. Algebra **36** (2008), no. 11, 4020–4031. MR 2460400

[2] S. Akbari, M. Ghandehari, M. Hadian, and A. Mohammadian, *On commuting graphs of semisimple rings*, Linear Algebra Appl. **390** (2004), 345–355. MR 2083665

[3] S. Akbari, M. Habibi, A. Majidinya, and R. Manaviyat, *The inclusion ideal graph of rings*, Comm. Algebra **43** (2015), no. 6, 2457–2465. MR 3344200

[4] S. Akbari, A. Mohammadian, H. Radjavi, and P. Raja, *On the diameters of commuting graphs*, Linear Algebra Appl. **418** (2006), no. 1, 161–176. MR 2257587

[5] C. Ambrozie, J. Bračič, B. Kuzma, and V. Müller, *The commuting graph of bounded linear operators on a Hilbert space*, J. Funct. Anal. **264** (2013), no. 4, 1068–1087. MR 3004958

[6] D.F. Anderson and A. Badawi, *The total graph of a commutative ring*, J. Algebra **320** (2008), no. 7, 2706–2719. MR 2441996

[7] D.F. Anderson and J.D. LaGrange, *Some remarks on the compressed zero-divisor graph*, J. Algebra **447** (2016), 297–321. MR 3427636

[8] D.F. Anderson and P.S. Livingston, *The zero-divisor graph of a commutative ring*, J. Algebra **217** (1999), no. 2, 434–447. MR 1700509

[9] J. Araújo, M. Kinyon, and J. Konieczny, *Minimal paths in the commuting graphs of semigroups*, European J. Combin. **32** (2011), no. 2, 178–197. MR 2738539

[10] C. Balbuena, *Incidence matrices of projective planes and of some regular bipartite graphs of girth 6 with few vertices*, SIAM J. Discrete Math. **22** (2008), no. 4, 1351–1363. MR 2443118

[11] L.M. Batten, *Combinatorics of finite geometries*, second ed., Cambridge University Press, Cambridge, 1997. MR 1474497

[12] N. Bloomfield and C. Wickham, *Local rings with genus two zero divisor graph*, Comm. Algebra **38** (2010), no. 8, 2965–2980. MR 2730289

[13] I.-V. Boroja, H.R. Dorbidi, D. Kokol Bukovšek, and N. Stopar, *Compressed commuting graphs of matrix rings*, Linear and Multilinear Algebra (2025), 19 pp., https://doi.org/10.1080/03081087.2024.2447527.

[14] I.-V. Boroja, D. Kokol Bukovšek, and N. Stopar, *When does an infinite ring have a finite compressed commuting graph?*, J. Algebra Appl. (2025), 2650148, https://doi.org/10.1142/S0219498826501483.

[15] R. Brauer and K.A. Fowler, *On groups of even order*, Ann. of Math. (2) **62** (1955), 565–583. MR 74414

[16] A. Djurić, S. Jevđenić, and N. Stopar, *Categorial properties of compressed zero-divisor graphs of finite commutative rings*, J. Algebra Appl. **20** (2021), no. 5, Paper No. 2150069, 16. MR 4255745

[17] ———, *Compressed zero-divisor graphs of matrix rings over finite fields*, Linear Multilinear Algebra **69** (2021), no. 11, 2012–2039. MR 4283119

[18] G. Dolinar, A. Guterman, B. Kuzma, and P. Oblak, *Extremal matrix centralizers*, Linear Algebra Appl. **438** (2013), no. 7, 2904–2910. MR 3018047

[19] ———, *Commuting graphs and extremal centralizers*, Ars Math. Contemp. **7** (2014), no. 2, 453–459. MR 3240449

[20] D. Dolžan, *The commuting graphs of finite rings*, Publ. Math. Debrecen **95** (2019), no. 1-2, 123–131. MR 3998029

[21] D. Dolžan, D. Kokol Bukovšek, and B. Kuzma, *On the lower bound for diameter of commuting graph of prime-square sized matrices*, Filomat **32** (2018), no. 17, 5993–6000. MR 3899333

[22] D. Dolžan, D. Kokol Bukovšek, and B. Kuzma, *On diameter of components in commuting graphs*, Linear Algebra Appl. **522** (2017), 161–174. MR 3621183

[23] H.R. Dorbidi, *On a conjecture about the commuting graphs of finite matrix rings*, Finite Fields Appl. **56** (2019), 93–96. MR 3883282

[24] H.R. Dorbidi and R. Manaviyat, *The commuting graph of the ring $M_3(F_q)$*, Linear Multilinear Algebra **72** (2024), no. 1, 25–30. MR 4685140

[25] A. Erfanian, K. Khashyarmanesh, and Kh. Nafar, *Non-commuting graphs of rings*, Discrete Math. Algorithms Appl. **7** (2015), no. 3, 1550027, 7. MR 3402835

[26] I.N. Herstein, *Abstract algebra*, Third ed., Prentice Hall, Inc., Upper Saddle River, NJ, 1996. MR 1375019

[27] T.W. Hungerford, *Algebra*, Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974. MR 354211

[28] A. Iranmanesh and A. Jafarzadeh, *Characterization of finite groups by their commuting graph*, Acta Math. Acad. Paedagog. Nyházi **23** (2007), no. 1, 7–13. MR 2322896

[29] ———, *On the commuting graph associated with the symmetric and alternating groups*, J. Algebra Appl. **7** (2008), no. 1, 129–146. MR 2386915

[30] N. Jacobson, *Lectures in abstract algebra. Vol. II. Linear algebra*, D. Van Nostrand Co., Inc., Toronto-New York-London, 1953. MR 0053905

[31] R. Kaye and R. Wilson, *Linear algebra*, Oxford Science Publications, Oxford University Press, Oxford, 1998. MR 1618277

[32] B. Kuzma, *Dimensions of complex Hilbert spaces are determined by the commutativity relation*, J. Operator Theory **79** (2018), no. 1, 201–211. MR 3764148

[33] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, First ed., Cambridge University Press, Cambridge, 1994. MR 1294139

[34] X. Ma and P.J. Cameron, *Finite groups whose commuting graph is split*, Tr. Inst. Mat. Mekh. **30** (2024), no. 1, 280–283. MR 4730001

[35] A. Mohammadian, *On commuting graphs of finite matrix rings*, Comm. Algebra **38** (2010), no. 3, 988–994. MR 2650384

[36] G.L. Morgan and C.W. Parker, *The diameter of the commuting graph of a finite group with trivial centre*, J. Algebra **393** (2013), 41–59. MR 3090056

[37] S.B. Mulay, *Cycles and symmetries of zero-divisors*, Comm. Algebra **30** (2002), no. 7, 3533–3558. MR 1915011

[38] S.P. Redmond, *The zero-divisor graph of a non-commutative ring*, Internat. J. Commutative Rings **1** (2002), no. 4, 203–211. MR 2037657

[39] Y. Shitov, *A matrix ring with commuting graph of maximal diameter*, J. Combin. Theory Ser. A **141** (2016), 127–135. MR 3479240

[40] D. Wang and C. Xia, *Diameters of the commuting graphs of simple Lie algebras*, J. Lie Theory **27** (2017), no. 1, 139–154. MR 3518119

[41] H. Zhang, *Automorphism group of the commuting graph of* 2×2 *matrix ring over* $\mathbb{Z}_{p^s}$, AIMS Math. **6** (2021), no. 11, 12650–12659. MR 4311374

Ivan Vanja Boroja

Personal data

Born on July 21st, 1978, in Mrkonjic Grad. Permanently residing in Bjelajce, Mrkonjic Grad, Republika Srpska, Bosnia and Herzegovina. Married to Bojana Boroja, a professor of Serbian language and literature. We have four children: Kristina (12 years old), Simona (7), Novak (5), and Ljubica (2).

Education

- 1985-1993. Primary School "Branko Copic"Bjelajce
- 1993-1997. Grammar School Mrkonjić Grad / Grammar School Podgorica
- 2005. Graduated Mathematician, Faculty of Natural Sciences and Mathematics in Podgorica
- 2015. Master of Computer Sciences, Faculty of Natural Sciences and Mathematics, Podgorica
- 2019 - Student of doctoral studies, Студент докторских студија, Faculty of Natural Sciences and Mathematics, Banja Luka

Professional Career

- 2010. - 2025. Employed at the University of Banja Luka (Faculty of Electrical Engineering, Faculty of Natural Sciences and Mathematics, Faculty of Architecture, Civil Engineering and Geodesy, Faculty of Mechanical Engineering, Faculty of Medicine)
- 2009. - 2010. Mathematics Teacher at the Grammar School
- 2005. - 2009. I worked as GIS technician for UNDP
- 2003. - 2005. IT technician, Embassy of France in Serbia and Montenegro

Foreign languages

- **English**
  Actively proficient in English, C1 level

- **French**
  Basic passive knowledge of French, A2 level
- **Russian**
  Elementary level (basic knowledge), level A1

Bibliography

- Boroja, Ivan-Vanja; Kokol Bukovšek, Damjana; Stopar, Nik When does an infinite ring have a finite compressed commuting graph? J. Algebra Appl., in press (2025), art. 2650148, 18 pp.
- Boroja, Ivan-Vanja; Dorbidi, Hamid Reza; Kokol Bukovšek, Damjana; Stopar, Nik Compressed commuting graphs of matrix rings. Linear Multilinear Algebra, in press (2025), 19 pp.
- D. Bogdanić, I.-V. Boroja Indecomposable Modules in the Grassmannian Cluster Category $CM(B_{(}5,10))$, Kragujevac Journal of Mathematics,Volume 48(6) (2024), Pages 907–920 https://imi.pmf.kg.ac.rs/kjm/en/index.php?page=accepted-papers
- D. Bogdanić, I.-V. Boroja Decomposable extensions between rank 1 modules in Grassmannian cluster category, Sarajevo Journal of Mathematics, Vol.18 (31), No.2 (2022), 297 – 312 DOI: 10.5644/SJM.18.02.10
- S. Maksimović, S. Kosić-Jeremić, I.-V. Boroja, N. Đurić Some recurrence formulas for a new class of special polynomials and special functions, STEPGRAD 2020 conference https://stepgrad.aggf.unibl.org/sr/novosti-i-najave/55-zbornik-radova

The rest

- Member of the Hunting Association "Lisina"Mrkonjić Grad; I served one term as Vice President of the Assembly of the Association.
- Member of the Mathematical Society of the city of Banja Luka; served one term on the Management Board.
- President of the Management Board of the City Library Mrkonjic Grad, two terms.
- Member of the School Board of the Mechanical School in Mrkonjic Grad, currently serving the third term.
- President of the Supervisory Board of the Public Enterprise "Hydroelectric Power Plants on the Vrbas."

Прилог 3.

Изјава 1

ИЗЈАВА О АУТОРСТВУ

Изјављујем
да је докторска дисертација

Наслов рада Компресовани графови комутативности прстена и других алгебарских структура

Наслов рада на енглеском језику Compressed commuting graphs of rings and other algebraic structures

☒ резултат сопственог истраживачког рада,

☒да докторска дисертација, у цјелини или у дијеловима, није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,

☒ да су резултати коректно наведени и

☒ да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанта
Иван Вања Бороја, с.р.

У Бањој Луци, дана 19. јуна 2025. године

Изјава 2

Изјава којом се овлашћује Универзитет у Бањој Луци да докторску дисертацију учини јавно доступном

Овлашћујем Универзитет у Бањој Луци да моју докторску дисертацију под насловом
Компресовани графови комутативности прстена и других алгебарских структура

која је моје ауторско дјело, учини јавно доступном.

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

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

- ○ Ауторство
- ○ Ауторство – некомерцијално
- ○ Ауторство – некомерцијално – без прераде
- ● Ауторство – некомерцијално – дијелити под истим условима
- ○ Ауторство – без прераде
- ○ Ауторство – дијелити под истим условима

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

Потпис докторанта

У Бањој Луци, дана 19.јуна 2025. године

Иван Вања Бороја, с.р.

____

ТИПОВИ ЛИЦЕНЦИ КРЕАТИВНЕ ЗАЈЕДНИЦЕ

Ауторство (CC BY)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дјела, и прераде, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

Ауторство - некомерцијално (CC BY-NC)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дјела и прераде, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дјела.

Ауторство - некомерцијално - без прерада (CC BY-NC-ND)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дјела, без промјена, преобликовања или употребе дјела у свом дијелу, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дјела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дјела.

Ауторство - некомерцијално - дијелити под истим условима (CC BY-NC-SA)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дијела, и прераде, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце, и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дјела и прерада

Ауторство - без прерада (CC BY-ND)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дјела, без промјена, преобликовања или употребе дјела у свом дјелу, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дјела.

Ауторство - дијелити под истим условима (CC BY-SA)

Дозвољавате умножавање, дистрибуцију и јавно саопштавање дјела, и прераде, ако се наведе име аутора, на начин одређен од аутора или даваоца лиценце, и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дјела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.

Напомена: Овај текст није саставни дио изјаве аутора.

Више информација на линку: *http://creativecommons.org.rs/*

Изјава 3

Изјава о идентичности штампане и електронске верзије докторске дисертације

Име и презиме аутора Иван Вања Бороја

Наслов рада Компресовани графови комутативности прстена и других алгебарских структура

Ментор Др Ник Стопар

Изјављујем да је штампана верзија моје докторске дисертације идентична електронској верзији коју сам предао/ла за дигитални репозиторијум Универзитета у Бањој Луци.

Потпис докторанта
Иван Вања Бороја, с.р.

У Бањој Луци, дана 19. јуна 2025. године

УНИВЕРЗИТЕТ У БАЊОЈ ЛУЦИ *Образац 3*
ЧЛАНИЦА: Природно-математички факултет

ИЗВЈЕШТАЈ

за оцјену урађене докторске дисертације / докторског умјетничког рада[1]

1. ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију: Научно-наставно вијеће Природно-математичког факултета

Датум именовања комисије: 14. мај 2025.

Број одлуке: 19-3.65/25

Чланови комисије:

1. Николић Бојан | доцент
Презиме и име | Звање
Математика, Алгебра и геометрија
Научно поље и ужа научна/умјетничка област
Природно-математички факултет, Унив. у Бањој Луци | предсједник
Установа у којој је запослен/а | Функција у комисији

2. Божовић Владимир | редовни професор
Презиме и име | Звање
Математика, Алгебра и геометрија
Научно поље и ужа научна/умјетничка област
Природно-математички факултет, Унив. Црне Горе | члан
Установа у којој је запослен/а | Функција у комисији

3. Кокол Буковшек Дамјана | ванредни професор
Презиме и име | Звање
Математика, Алгебра и геометрија
Научно поље и ужа научна/умјетничка област
Економски факултет, Унив. у Љубљани | члан
Установа у којој је запослен/а | Функција у комисији

4. Димитрије Чвокић | доцент
Презиме и име | Звање
Информационе науке, Информационе науке и биоинформатика (развој софтвера)
Научно поље и ужа научна/умјетничка област
Природно-математички факултет, Унив. у Бањој Луци | члан
Установа у којој је запослен/а | Функција у комисији

5.
Презиме и име | Звање

[1] У даљем тексту „дисертација / умјетнички рад".

Научно поље и ужа научна/умјетничка област

Установа у којој је запослен/а

Функција у комисији

2. ПОДАЦИ О СТУДЕНТУ

Име, име једног родитеља, презиме: Иван Вања (Митар) Бороја

Датум рођења: 21. јул 1978.

Мјесто и држава рођења: Мркоњић Град, Република Српска, Босна и Херцеговина

2.1. Студије првог циклуса или основне студије или интегрисане студије

Година уписа:	1997.	Година завршетка:	2005.	Просјечна оцјена током студија:	9,00

Универзитет: Универзитет Црне Горе

Факултет/Академија: Природно-математички факултет

Студијски програм: Математика

Стечено звање: Дипломирани математичар, број дипломе 245. Рјешењем Министарства просвјете и културе Републике Српске број 07.023/613-509/14 од 3. новембра 2014. диплома је нострификована.

2.2. Студије другог циклуса или мастер студије

Година уписа:	2014.	Година завршетка:	2015.	Просјечна оцјена током студија:	9,80

Универзитет: Универзитет Црне Горе

Факултет/Академија: Природно-математички факултет

Студијски програм: Примијењена математика и рачунарске науке

Назив завршног рада другог циклуса или мастер тезе, датум одбране:

„Алгоритми за конструкцију репрезентација и карактера семи-директног производа група“, Подгорица, 30. април 2015.

Ужа научна/умјетничка област завршног рада другог циклуса или мастер тезе:

Рачунарске науке

Стечено звање: Магистар

2.3. Студије трећег циклуса

Година уписа:	2019.	Број ECTS бодова остварених до сада:	135	Просјечна оцјена током студија:	10.00

Факултет/Академија: Природно-математички факултет, Универзитет у Бањој Луци

Студијски програм: Математика

2.4. Приказ научних и стручних односно умјетничких радова студента[2]

Навести појединачне радове, са навођењем DOI бројева, односно концерте / снимљена дјела. Додати потребан број редова. Користити исти стил за навођење свих референци у 2.4.

Р.б.	Основни подаци о научном раду	Цитатна база
1.	**Boroja, Ivan-Vanja**; Kokol Bukovšek, Damjana; Stopar, Nik *When does an infinite ring have a finite compressed commuting graph?* J. Algebra Appl., in press (2025), art. 2650148, 18 pp.	Web of Science Core Collection
2.	**Boroja, Ivan-Vanja**; Dorbidi, Hamid Reza; Kokol Bukovšek, Damjana; Stopar, Nik *Compressed commuting graphs of matrix rings.* Linear Multilinear Algebra, in press (2025), 19 pp.	Web of Science Core Collection
3.	Bogdanić, Duško; **Boroja, Ivan-Vanja,** *Indecomposable Modules in the Grassmannian Cluster Category CM(B_(5,10))*, Kragujevac Journal of Mathematics, Volume 48(6) (2024), Pages 907–920 https://imi.pmf.kg.ac.rs/kjm/en/index.php?page=accepted-papers	Web of Science Core Collection
4.	Bogdanić, Duško; **Boroja, Ivan-Vanja,** *Decomposable extensions between rank 1 modules in Grassmannian cluster category*, Sarajevo Journal of Mathematics, Vol.18 (31), No.2 (2022), 297 – 312 DOI: 10.5644/SJM.18.02.10	-------------------
5.		Изабери ...

Припадност рада ужој научној/умјетничкој области којој припада предмет истраживања докторске дисертације ☑ ДА □ НЕ

3. УВОДНИ ДИО ОЦЈЕНЕ ДИСЕРТАЦИЈЕ / УМЈЕТНИЧКОГ РАДА

1. Компресовани графови комутативности прстена и других алгебарских структура
2. Математика, Алгебра и геометрија
3. 24. октобар 2024. Одлука Сената Универзитета у Бањој Луци број 02/04-3.2250-79/24
4. 26. децембар 2024. Одлука Сената Универзитета у Бањој Луци број 02/04-3.2747-49/24
5. Дисертација је написана на 87 страница, од чега главни дио рада обухвата 77 страница, подијељених на 10 поглавља:
    1. Увод (странице 1-4)
    2. Припремна разматрања (странице 5-14)
    3. Компресовани граф комутативности прстена са јединицом (странице 15-18)
    4. Компресовани граф комутативности прстена $\mathrm{M}_2(GF(p))$ (странице 19-28)
    5. Скуп чворова компресованог графа комутативности $\Lambda^1(\mathrm{M}_3(GF(p)))$ (странице 29-46)
    6. Сусједи чворова графа $\Lambda^1(\mathrm{M}_3(GF(p)))$ (странице 47-60)
    7. Подграф индукован скупом чворова $V_{(B)} \cup V_{(E)}$ (странице 61-68)
    8. Опис графа $\Lambda^1(\mathrm{M}_3(GF(p)))$ (странице 69-72)
    9. Граф комутативности прстена $\mathrm{M}_3(GF(p)$ (страница 73)
    10. Литература (странице 74-77)
6. Дисертација је написана на енглеском језику, има 87 страница А4 формата и подељена је у 10 поглавља. Почиње уводом који описује тренутно стање у области, циљеве и структуру

[2] У складу са чланом 34 Правила студирања на трећем циклусу студија, септембра 2022. године.

дисертације. Поглавље о прелиминарним резултатима подсјећа на неколико резултата из теорије матрица који су коришћени у дисертацији. Треће поглавље уводи главни објекат истраживања и сумира нека позната истраживања. Граф прстена матрица 2x2 над простим пољем описује се у четвртом поглављу, док се граф прстена матрица 3x3 над простим пољем описује у поглављима 5-8, почевши од поглавља о тјеменима, поглавља о комшилуцима, и два поглавља која описују граф у целини. Дисертација наставља деветим поглављем, које даје опис уобичајеног графа комутативности прстена матрица 3x3 над простим пољем као примјену. Десето поглавље је библиографија која садржи 41 референцу. Дисертација садржи 13 табела и једну слику.

1. Наслов дисертације / умјетничког рада.
2. Научно поље и ужа научна/умјетничка област.
3. Датум прихватања теме дисертације / умјетничког рада и бројеви одлука одговарајућих органа чланица и Универзитета.
4. Датум прихватања извјештаја комисије за оцјену подобности студента, теме и ментора за израду дисертације / умјетничког рада и бројеви одлука одговарајућих органа чланица и Универзитета.
5. Садржај дисертације / умјетничког рада уз навођење броја страна.
6. Истаћи основне податке о дисертацији / умјетничком раду: обавезно укључујући обим, број и називе поглавља, број табела, слика, шема, графикона и број литературних навода.

4. УВОД И ПРЕГЛЕД ЛИТЕРАТУРЕ

1. Представљање проблема: Посљедњих година, велики број истраживања посвећен је разним графовима индукованим алгебарским структурама, као што су прстенови, групе итд. Ово истраживање је фокусирано на употребу алата из теорије графова за истраживање структурних својстава алгебарских структура. Један од најважнијих примјера је граф комутативности прстена, који приказује релацију комутативности. Значај овог приступа је очигледан из бројних нових резултата о централизаторима и комутативности у прстеновима матрица које је произвео, јер представљање комутативности графом даје истраживачима вриједне увиде у својства која би иначе остала невидљива. Даљи напредак постигнут је у случају графа дјелилаца нуле прстена, гдје је оригинални граф компресован како би постао мањи и тиме лакши за управљање. Недавно је уведен нови тип компресованог графа дјелилаца нуле прстена, који показује много боље везе са структуром прстена, углавном због чињенице да индукује функтор из категорије прстенова у категорију графова. Ова компресија још увек није истражена у случају графа комутативности.

Предмет истраживања: Граф комутативности и компресовани граф комутативности који описују релацију комутативности између елемената алгебарске структуре.

Циљ истраживања: Један од првих циљева истраживања је проширење методе са графова дјелилаца нуле на графове комутативности и увођење компресије графа комутативности прстена која индукује функтор. Други циљ је истраживање својстава уведеног графа, нарочито да се одговори на питање да ли бесконачан прстен може имати коначан компресовани граф комутативности и када се то дешава. Главни циљ дисертације је истраживање компресованог графа комутативности прстена матрица реда 2 и 3 над простим пољем GF(p) за било који дати прост број p. Сви ови циљеви су постигнути, а резултати су концизно представљени у дисертацији.

Хипотезе истраживања:
1. За граф комутативности алгебарске структуре могуће је пронаћи компресију која даје најмањи могући граф такав да су испоштована функторијална својства одговарајуће алгебарске структуре.
2. Бесконачна алгебарска структура може имати коначан компресовани граф комутативности.

3. Одређене важне фамилије графова као што су потпуни графови, звјездасти графови и др. могу бити компресовани графови комутативности неке алгебарске структуре.

4. Неки прстени и алгебре су до на изоморфизам јединствено одређени својим компресованим графом комутативности, као на примјер прстен матрица 2x2 над пољем Галоа са p елемената, гдје је p прост број.

5. Могуће је у потпуности описати компресовани граф комутативности алгебре матрица малог реда над пољем мале кардиналности.

У дисертацији је потврђена већина наведених хипотеза. Прва, друга, други дио четврте и пета хипотеза су у потпуности потврђене док су трећа и први дио четврте хипотезе верификовани у пратећим радовима кандидата.

2. Преглед литературе:

[1] S. Akbari, H. Bidkhori, and A. Mohammadian, Commuting graphs of matrix algebras, Comm. Algebra 36 (2008), no. 11, 4020–4031. MR 2460400

[2] S. Akbari, M. Ghandehari, M. Hadian, and A. Mohammadian, On commuting graphs of semisimple rings, Linear Algebra Appl. 390 (2004), 345–355. MR 2083665

[3] S. Akbari, M. Habibi, A. Majidinya, and R. Manaviyat, The inclusion ideal graph of rings, Comm. Algebra 43 (2015), no. 6, 2457–2465. MR 3344200

[4] S. Akbari, A. Mohammadian, H. Radjavi, and P. Raja, On the diameters of commuting graphs, Linear Algebra Appl. 418 (2006), no. 1, 161–176. MR 2257587

[5] C. Ambrozie, J. Bračič, B. Kuzma, and V. Müller, The commuting graph of bounded linear operators on a Hilbert space, J. Funct. Anal. 264 (2013), no. 4, 1068–1087. MR 3004958

[6] D.F. Anderson and A. Badawi, The total graph of a commutative ring, J. Algebra 320 (2008), no. 7, 2706–2719. MR 2441996

[7] D.F. Anderson and J.D. LaGrange, Some remarks on the compressed zero-divisor graph, J. Algebra 447 (2016), 297–321. MR 3427636

[8] D.F. Anderson and P.S. Livingston, The zero-divisor graph of a commutative ring, J. Algebra 217 (1999), no. 2, 434–447. MR 1700509

[9] J. Araújo, M. Kinyon, and J. Konieczny, Minimal paths in the commuting graphs of semigroups, European J. Combin. 32 (2011), no. 2, 178–197. MR 2738539

[10] C. Balbuena, Incidence matrices of projective planes and of some regular bipartite graphs of girth 6 with few vertices, SIAM J. Discrete Math. 22 (2008), no. 4, 1351–1363. MR 2443118

[11] L.M. Batten, Combinatorics of finite geometries, second ed., Cambridge University Press, Cambridge, 1997. MR 1474497

[12] N. Bloomfield and C. Wickham, Local rings with genus two zero divisor graph, Comm. Algebra 38 (2010), no. 8, 2965–2980. MR 2730289

[13] I.-V. Boroja, H.R. Dorbidi, D. Kokol Bukovšek, and N. Stopar, Compressed commuting graphs of matrix rings, Linear and Multilinear Algebra (2025), 19 pp., https://doi.org/10.1080/03081087.2024.2447527.

[14] I.-V. Boroja, D. Kokol Bukovšek, and N. Stopar, When does an infinite ring have a finite compressed commuting graph?, J. Algebra Appl. (2025), 2650148,

https://doi.org/10.1142/S0219498826501483.

[15] R. Brauer and K.A. Fowler, On groups of even order, Ann. of Math. (2) 62 (1955), 565–583. MR 74414

[16] A. Djurić, S. Jevđenić, and N. Stopar, Categorial properties of compressed zero-divisor graphs of finite commutative rings, J. Algebra Appl. 20 (2021), no. 5, Paper No. 2150069, 16. MR 4255745

[17] , Compressed zero-divisor graphs of matrix rings over finite fields, Linear Multilinear Algebra 69 (2021), no. 11, 2012–2039. MR 4283119

[18] G. Dolinar, A. Guterman, B. Kuzma, and P. Oblak, Extremal matrix centralizers, Linear Algebra Appl. 438 (2013), no. 7, 2904–2910. MR 3018047

[19] , Commuting graphs and extremal centralizers, Ars Math. Contemp. 7 (2014), no. 2, 453–459. MR 3240449

[20] D. Dolžan, The commuting graphs of finite rings, Publ. Math. Debrecen 95 (2019), no. 1-2, 123–131. MR 3998029

[21] D. Dolžan, D. Kokol Bukovšek, and B. Kuzma, On the lower bound for diameter of commuting graph of prime-square sized matrices, Filomat 32 (2018), no. 17, 5993–6000. MR 3899333

[22] D. Dolžan, D. Kokol Bukovšek, and B. Kuzma, On diameter of components in commuting graphs, Linear Algebra Appl. 522 (2017), 161–174. MR 3621183

[23] H.R. Dorbidi, On a conjecture about the commuting graphs of finite matrix rings, Finite Fields Appl. 56 (2019), 93–96. MR 3883282

[24] H.R. Dorbidi and R. Manaviyat, The commuting graph of the ring M3(Fq), Linear Multilinear Algebra 72 (2024), no. 1, 25–30. MR 4685140

[25] A. Erfanian, K. Khashyarmanesh, and Kh. Nafar, Non-commuting graphs of rings, Discrete Math. Algorithms Appl. 7 (2015), no. 3, 1550027, 7. MR 3402835

[26] I.N. Herstein, Abstract algebra, Third ed., Prentice Hall, Inc., Upper Saddle River, NJ, 1996. MR 1375019

[27] T.W. Hungerford, Algebra, Holt, Rinehart and Winston, Inc., New York-Montreal, Que.-London, 1974. MR 354211

[28] A. Iranmanesh and A. Jafarzadeh, Characterization of finite groups by their commuting graph, Acta Math. Acad. Paedagog. Nyházi 23 (2007), no. 1, 7–13. MR 2322896

[29] , On the commuting graph associated with the symmetric and alternating groups, J. Algebra Appl. 7 (2008), no. 1, 129–146. MR 2386915

[30] N. Jacobson, Lectures in abstract algebra. Vol. II. Linear algebra, D. Van Nostrand Co., Inc., Toronto-New York-London, 1953. MR 0053905

[31] R. Kaye and R. Wilson, Linear algebra, Oxford Science Publications, Oxford University Press, Oxford, 1998. MR 1618277

[32] B. Kuzma, Dimensions of complex Hilbert spaces are determined by the commutativity relation, J. Operator Theory 79 (2018), no. 1, 201–211. MR 3764148

[33] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, First ed.,

Cambridge University Press, Cambridge, 1994. MR 1294139

[34] X. Ma and P.J. Cameron, Finite groups whose commuting graph is split, Tr. Inst. Mat. Mekh. 30 (2024), no. 1, 280–283. MR 4730001

[35] A. Mohammadian, On commuting graphs of finite matrix rings, Comm. Algebra 38 (2010), no. 3, 988–994. MR 2650384

[36] G.L. Morgan and C.W. Parker, The diameter of the commuting graph of a finite group with trivial centre, J. Algebra 393 (2013), 41–59. MR 3090056

[37] S.B. Mulay, Cycles and symmetries of zero-divisors, Comm. Algebra 30 (2002), no. 7, 3533–3558. MR 1915011

[38] S.P. Redmond, The zero-divisor graph of a non-commutative ring, Internat. J. Commutative Rings 1 (2002), no. 4, 203–211. MR 2037657

[39] Y. Shitov, A matrix ring with commuting graph of maximal diameter, J. Combin. Theory Ser. A 141 (2016), 127–135. MR 3479240

[40] D. Wang and C. Xia, Diameters of the commuting graphs of simple Lie algebras, J. Lie Theory 27 (2017), no. 1, 139–154. MR 3518119

[41] H. Zhang, Automorphism group of the commuting graph of 2 × 2 matrix ring over Zps , AIMS Math. 6 (2021), no. 11, 12650–12659. MR 4311374

Резултати претходних истраживања:

Граф комутативности описује релацију комутативности између елемената алгебарске структуре А. По дефиницији, то је прости граф чији су чворови нецентрални елементи алгебарске структуре, а два различита чвора су повезана ако одговарајући елементи комутирају у А. Први пут појам графа комутативности се помиње 1955. године у раду [15], у покушају да се класификују коначне просте групе. Прије око 20 година, такође је дефинисан за прстене и друге алгебарске структуре, [2,1]. Од тада му истраживачи посвећују велику пажњу, проучавајући повезаност графа, дијаметар и друга својства, [4,21]. Важно питање у овој теорији је проблем изоморфизма, који поставља питање када су изоморфне алгебарске структуре ако су изоморфни одговарајући графови комутативности.

И друга својства алгебарских структура такође могу бити описана графовима. Тако су настали Кејлијев граф, граф дјелилаца нуле, генеришући граф, тотални граф [5] и сл.

Године 2002. у раду [37] уведен је појам компресованог графа дјелилаца нуле са циљем да се граф учини мањим и самим тим лакшим за истраживање, а да њим и даље буде описана структура дјелилаца нуле. У радовима [16, 17] из 2001. године презентован је модификовани начин компресије који узима у обзир не само прстене него и хомоморфизме између прстена.

2. Укратко описати разлоге због којих су истраживања предузета и представити проблем, предмет, циљеве и хипотезе[3].
3. На основу прегледа литературе, сажето приказати резултате претходних истраживања у вези проблема који је истраживан (водити рачуна о томе да обухвата најновија и најзначајнија сазнања из те области код нас и у свијету).
4. Навести допринос тезе у рјешавању изучаваног предмета истраживања.
5. Навести очекивани научни и практични односно умјетнички допринос дисертације.

[3] Хипотезе приказати само за научни докторат.

5. МАТЕРИЈАЛ И МЕТОДОЛОГИЈА РАДА

1. Материјали који су кориштени за истраживање су искључиво писани радови објављени у разним математичким часописима са SCI листе као и уџбеници реномираних универзитета, с обзиром да је истраживање из теоријске математике.

2. Дисертација користи широк спектар метода из различитих математичких области и комбинује их како би се постигао главни циљ. Ове области укључују теорију графова, теорију група, линеарну алгебру, теорију коначних поља, коначне пројективне просторе и комбинаторику. Ове области чине интегралне дијелове доказа главног резултата дисертације.

   Метода компресије и метода „проширења" графова прилагођене су из случаја графа делилаца нуле прстена. Тјемена графа $\Lambda^1(\mathrm{M}_3\big(GF(p)\big)$ тј. компресованог графа комутативности прстена матрица 3x3 над простим пољем GF(p) су описана разматрањем случајева заснованих на сличности матрица. Главни алати који су коришћени током овог корака били су алати линеарне алгебре, као што су сопствене вредности и сопствени вектори, линеарни простори и њихове димензије и Жорданова форма матрице. Такође је било потребно познавање теорије коначних поља и употреба полинома. За сваки чвор графа, скуп његових сусједа истраживан је коришћењем матричног рачуна и комбинаторике. Језгро графа $\Lambda^1(\mathrm{M}_3(GF(p))$ описано је успостављањем бијекције између чворова графа и парова тачака-линија у пројективној равни над GF(p), ослањајући се на матрицу инциденције.

   a. Примијењене методе истраживања су адекватне, јер су резултирале рјешењем проблема описа графа комутативности прстена матрица 3x3.
   b. Првобитни план истраживања спроведен је у цјелости.
   c. Спроведени обим истраживања је довољан за доношење поузданих закључака.
   d. У истраживању није коришћена статистичка обрада резултата.

1. Описати и дати основне карактеристике материјала који је обрађиван, критеријуме који су узети у обзир за избор материјала.
2. Дати кратак увид у примијењени метод истраживања, при чему је важно оцијенити сљедеће:
   a. Да ли су примијењене методе истраживања адекватне, довољно тачне и савремене, имајући у виду достигнућа на том пољу у свјетском оквиру;
   b. Образложити евентуалне измјене првобитног плана истраживања;
   c. Да ли је обим истраживања довољан за доношење поузданих закључака или је потребно проширити постојеће или увести нове методе;
   d. Да ли је статистичка обрада података адекватна, ако је коришћена при обради резултата.

6. РЕЗУЛТАТИ И НАУЧНИ/УМЈЕТНИЧКИ ДОПРИНОС ИСТРАЖИВАЊА

1. Главни доприноси истраживања су следећи:

   - Потпун опис компресованог графа комутативности прстена матрица 3x3 над простим пољем GF(p), уз алгоритам за његову конструкцију.

   - Опис уобичајеног графа комутативности прстена матрица 3x3 над простим пољем GF(p). Ово је било отворено питање од момента увођења графа комутативности.

   - Увођење новог типа графа индукованог прстеном, тј. компресованог графа комутативности.

   - Унапређење метода коришћених за опис компресованог графа комутативности прстена матрица 2x2 над пољем GF(p).

2. Резултати су јасно приказани, правилно, логично и јасно тумачени. Довољан ниво критичности потврђује чињеница да је студент спровео студиозно истраживање ове тематике што је резултовало објављивањем два рада у часописима на SCI листи.
3. Резултати дисертације могу се показати корисним у будућим истраживањима. Конкретно, развијене методе помоћи ће да се генерализују резултати на матрице вишег реда над генералнијим пољима. Такође, резултати би могли бити употријебљени за покушај рјешавања проблема изоморфизма за прстенове матрица.

1. Укратко навести резултате до којих је студент дошао.
2. Оцијенити да ли су добијени резултати јасно приказани, правилно, логично и јасно тумачени, упоређујући их са резултатима других аутора и да ли је студент при томе испољавао довољно критичности.
3. Посебно је важно истаћи до којих нових сазнања се дошло у истраживању, који је њихов теоријски и практични допринос, те да ли указују на нове правце истраживања.

7. ЗАКЉУЧАК И ПРИЈЕДЛОГ

1. Кандидат је истраживао актуелан проблем и добијени резултати су коректно интерпретирани. Очекује се да новоразвијени компресовани граф комутативности подстакне нова истраживања у области прстена матрица и релације комутативности користећи алате теорије графова.
2. Будући да је кандидат показао темељно познавање предмета истраживања, те у потпуности одговорио на проблематику која се разматра у дисертацији, Комисија предлаже Научно-наставном вијећу Природно-математичког факултета Универзитета у Бањој Луци и Сенату Универзитета у Бањој Луци да се усвоји овај извјештај и докторска дисертација под називом ‘’Компресовани графови комутативности прстена и других алгебарских структура‘‘ кандидата мр. Ивана Вање Бороје прихвати, као и да се одобри јавна одбрана ове дисертације пред комисијом у истом саставу.

1. Навести најзначајније чињенице које указују на научни/уметнички допринос дисертације.
2. На основу укупне оцјене дисертације, комисија предлаже:
   - да се дисертација / умјетнички рад прихвати, а студенту одобри одбрана,
   - да се дисертација / умјетнички рад враћа студенту на дораду (да се допуни или измијени) или
   - да се дисертација / умјетнички рад одбија.

Мјесто и датум: У Бањој Луци, 27. маја 2025.

Бојан Николић, доц. др
Предсједник комисије

Владимир Божовић, ред. проф
Члан

Дамјана Кокол Буковшек, ван. проф
Члан

Димитрије Чвокић,доц. др
Члан

____

Име и презиме, титула и звање

Члан

ИЗДВОЈЕНО МИШЉЕЊЕ: Члан комисије који не жели да потпише извјештај јер се не слаже са мишљењем већине чланова комисије дужан је да у извјештај унесе образложење, то јест разлоге због којих не жели да потпише извјештај.

У прилогу извјештаја доставити:

1. Одлуку Умјетничко-научно-наставног / научно-наставног вијећа чланице Универзитета о именовању комисије за оцјену урађене докторске дисертације / докторског умјетничког рада и јавну одбрану;
2. Одлуку Умјетничко-научно-наставног / научно-наставног вијећа чланице Универзитета о прихватању извјештаја комисије за оцјену урађене докторске дисертације / докторског умјетничког рада и јавну одбрану;
3. Извјештај комисије за оцјену урађене докторске дисертације / докторског умјетничког рада и јавну одбрану – Образац 3;
4. Докторска дисертација у ПДФ формату;
5. Увјерење продекана за научноистраживачки рад и развој о провјери оригиналности докторске дисертације путем званичног софтвера за откривање плагијаризма;
6. Изјава о ауторству;
7. Изјава којом се овлашћује Универзитет у Бањој Луци да докторску дисертацију / докторски умјетнички рад учини јавно доступним;
8. Изјава о идентичности штампане и електронске верзије докторске дисертације / докторског умјетничког рада.