Research article

Automorphism group of the commuting graph of $2 \times 2$ matrix ring over $\mathbb{Z}_{p^s}$

Hengbin Zhang

College of Mathematical Science, Yangzhou University, Yangzhou, Jiangsu 225009, China

* Correspondence: Email: hengbinzhang@yzu.edu.cn.

Abstract: Let $R$ be a ring with identity. The commuting graph of $R$ is the graph associated to $R$ whose vertices are non-central elements in $R$, and distinct vertices $A$ and $B$ are adjacent if and only if $AB = BA$. In this paper, we completely determine the automorphism group of the commuting graph of $2 \times 2$ matrix ring over $\mathbb{Z}_{p^s}$, where $\mathbb{Z}_{p^s}$ is the ring of integers modulo $p^s$, $p$ is a prime and $s$ is a positive integer.

Keywords: commuting graph; automorphism group; matrix ring

Mathematics Subject Classification: 20B25, 15B33

1. Introduction

Let $R$ be a ring with identity, and let $C(R)$ be the center of $R$. The commuting graph $\Gamma(R)$ of $R$ is the graph associated to $R$ whose vertices are the elements of $R \setminus C(R)$ such that distinct vertices $A$ and $B$ are adjacent if and only if $AB = BA$. For the purpose of investigating the structures of a group or a ring, there are many associated graphs that have been studied extensively. Let $M_n(F)$ denote the ring of $n \times n$ matrices over $F$, where $F$ is a field and $n \geq 2$ an arbitrary integer. In [1], if $F$ is a finite field then $|\Gamma(M_n(F))| = |\Gamma(M_n(F))|$. Furthermore, if $F$ is a prime field and $n = 2$, then $\Gamma(M_2(F))$. In [2], this result still holds if it is just assumed that $F$ is a finite field. There are also some graph-theoretic properties of the commuting graphs that have been investigated, such as connectivity and domination number. In [3], Akbari et al. showed that $\Gamma(M_n(F))$ is a connected graph if and only if every field extension of $F$ of degree $n$ contains a proper intermediate field. Also it is shown that for two fields $F$ and $E$ and integers $n, m \geq 2$, if $\Gamma(M_n(F)) \equiv \Gamma(M_m(E))$, then $n = m$ and $|F| = |E|$.

The commuting graph of a finite group $\Delta(G)$ is the graph whose vertex set is $G$ with $x, y \in G$, $x \neq y$, joined by an edge whenever $xy = yx$, where $G$ is a finite group. The graph $\Delta(G)$ has been studied in [4–7]. The set of all automorphisms of a graph forms a group known as the graph’s automorphism group. The automorphism group of a graph describes its symmetries. In [6], it is proved that the automorphism group of $\Delta(G)$ is abelian if and only if $|G| \leq 2$. With the wreath product, Mirzargar
et al. [7] determined the automorphism group of $\Delta(G)$, where $G$ is an AC-group. In [8], it is proved that the automorphism group of $\Gamma(M_2(F))$ is a direct product of symmetric groups, where $F$ is a finite field. In this paper, motivated by these works, we extend the finite field to the ring of integers modulo $p^s$, and we completely determine the automorphism group of $\Gamma(M_2(\mathbb{Z}_{p^s}))$, where $\mathbb{Z}_{p^s}$ is the ring of integers modulo $p^s$, $p$ is a prime and $s$ is a positive integer. This paper is organized as follows. In section 2, we give some preliminaries, notation, lemmas and definition of the wreath product. In section 3, we show that the automorphism group of $\Gamma(M_2(\mathbb{Z}_{p^s}))$ is a subgroup of a direct product of some wreath products, and we completely characterize it in Theorem 3.8.

2. Preliminaries and notation

In this paper, let $M_2(\mathbb{Z}_{p^s})$ denote the $2 \times 2$ matrix ring over $\mathbb{Z}_{p^s}$, we write it $R$ for short. Let $E_{ij}$ denote the matrix in $R$ having 1 in its $(i, j)$ entry and zeros elsewhere, and let $E$ denote the identity matrix. It is well known that $C(R) = \{aE \mid a \in \mathbb{Z}_{p^s}\}$. For $A \in R$, $C_R(A) = \{B \in R \mid AB = BA\}$ is called the centralizer of $A$ in $R$. For the ring $R$, let us denote by $U(R)$ and $D(R)$ the unit group and the zero divisor set of $R$ respectively. The commuting graph of $R$ is the graph with vertices $R \setminus C(R)$, and distinct vertices $A$ and $B$ are adjacent if and only if $AB = BA$. In a graph $G$, if $x$ is adjacent to $y$ (denoted by $[x, y]$), then we say that $x$ is a neighbor of $y$ or that $y$ is a neighbor of $x$. Let $N(x)$ denote the neighbors of $x$ in $G$. A graph automorphism of a graph $G$ is a bijection on vertex set (denoted by $V(G)$) which preserves adjacency. For $a \in \mathbb{Z}_{p^s}$, let $\langle a \rangle$ be the ideal of $\mathbb{Z}_{p^s}$ generated by $a$, we will denote by $\text{Ann}(a)$ the set $\{b \in \mathbb{Z}_{p^s} \mid ab = 0\}$, and by $\text{Ass}(a)$ the set $\{ua \mid u \in U(\mathbb{Z}_{p^s})\}$. Write $T = \{0, 1, \cdots, p - 1\} \subseteq \mathbb{Z}_{p^s}$. The subset of $T$ consisting of all non-zero elements is denoted by $T^*$. Let us denote by $S_n$ the symmetric group of degree $n$. For a set $D$, we will denote by $|D|$ the size of $D$, and by $S_D$ the symmetric group on $D$.

Lemma 2.1. [9, p. 328] Every non-zero element in $\mathbb{Z}_{p^s}$ can be written uniquely as

$$t_0 + t_1p + \cdots + t_{s-1}p^{s-1},$$

where $t_i \in T$, $i \in \{0, 1, \cdots, s - 1\}$. Furthermore, $|\langle p^i \rangle| = p^{s-i}$, $|\text{Ass}(p^i)| = p^{s-i} - p^{s-i-1}$, and $\text{Ann}(p^i) = \langle p^{s-i} \rangle$.

Definition 2.2. [10, p. 172] Let $D$ and $Q$ be groups, let $\Omega$ be a finite $Q$-set, and let $K = \prod_{\omega \in \Omega} D_\omega$, where $D_\omega \cong D$ for all $\omega \in \Omega$. Then the wreath product of $D$ by $Q$, denoted by $D \wr Q$, is the semidirect product of $D$ by $Q$, where $Q$ acts on $K$ by $q \cdot (d_\omega) = (d_{q.\omega})$ for $q \in Q$ and $(d_\omega) \in \prod_{\omega \in \Omega} D_\omega$.

Lemma 2.3. ([10, p. 178] or [11, Theorem 2.1.6]) Let $X = B_1 \cup \cdots \cup B_m$ be a partition of a set $X$ in which each $B_i$ has $k$ elements. If $G = \{g \in S_X \mid$ for each $i$, there is $j$ with $g(B_i) = B_j\}$, then $G \cong S_k \wr \Omega_m,$ where $\Omega_m = \{1, 2, \cdots, m\}$.

Let $X = \bigcup_{i_1=1}^{m_1} B_{i_1}$ be a partition of a set $X$ in which each $B_{i_1}$ has same size. Let $B_{i_1} = \bigcup_{i_2=1}^{m_2} B_{i_1,i_2}$ be a partition of a set $B_{i_1}$ in which each $B_{i_1,i_2}$ has same size, where $i_1 = 1, 2, \cdots, m_1$. Continuing in this way we obtain partitions

$$X = \bigcup_{i_j=1}^{m_j} \cdots \bigcup_{i_1=1}^{m_1} B_{i_1,\cdots,i_j}$$

AIMS Mathematics Volume 6, Issue 11, 12650–12659.
of \( X \) in which each \( B_{1i, \ldots, j} \) has same size for \( j = 1, \ldots, k \). With this notation, by Lemma 2.3, we have the following:

**Corollary 2.4.** ([12, p. 93] or [11, Theorem 2.1.15]) Let \( G \) be the largest subgroup of \( S_X \) preserving above partitions and \( |B_{1i, \ldots, j}| = m_{k+1} \). Then \( G = \{ g \in S_X \mid \text{for each } i_j, \text{there is } i'_j \text{ with } g(B_{1i, \ldots, j}) = B_{i'_j, \ldots, j}, j = 1, \ldots, k \} \). Moreover, \( G \cong \left( \cdots (S_{m_{k+1}} \circ \Omega_{m_k}) \cdots \circ \Omega_{m_2} \right) \circ \Omega_{m_1} \), where \( \Omega_{m_i} = \{ 1, 2, \ldots, m_i \} \) for \( i = 1, 2, \ldots, k+1 \).

With the associativity of the wreath product (see [10, Theorem 7.26]), we will simply write \( \left( \cdots (S_{m_{k+1}} \circ \Omega_{m_k}) \cdots \circ \Omega_{m_2} \right) \circ \Omega_{m_1} \) as \( S_{m_{k+1}} \circ \Omega_{m_k} \cdots \circ \Omega_{m_2} \circ \Omega_{m_1} \). In [11, p. 68], the iterated wreath product \( S_{m_{k+1}} \circ \Omega_{m_k} \cdots \circ \Omega_{m_2} \circ \Omega_{m_1} \) consists of all \( f_{k+1} \circ f_k \circ \cdots \circ f_2 \circ f_1 \), where \( f_i \in S_{m_i} \) and

\[
f_j = \prod_{i_j=1}^{m_{j-1}} \prod_{i_{j-2}=1}^{m_{j-2}} \cdots \prod_{i_1=1}^{m_1} g_{j, j-1, \ldots, j_2, j_1}, \quad j = 2, 3, \ldots, k+1,
\]

with the action on \( \prod_{j=1}^{k+1} \Omega_{m_j} \) defined by

\[
(f_{k+1} \circ f_k \circ \cdots \circ f_2 \circ f_1)(x_1, x_2, \ldots, x_{k+1}) = (y_1, y_2, \ldots, y_{k+1}),
\]

where \( y_j = f_j(x_j) \) and \( y_j = g_{j, y_{j-1} \ldots, j_2, j_1}(x_j), j = 2, 3, \ldots, k+1 \) for all \( (x_1, x_2, \ldots, x_{k+1}) \in \prod_{j=1}^{k+1} \Omega_{m_j} \) and \( f_{k+1} \circ f_k \circ \cdots \circ f_2 \circ f_1 \in S_{m_{k+1}} \circ \Omega_{m_k} \cdots \circ \Omega_{m_2} \circ \Omega_{m_1} \).

3. **Automorphisms of \( \Gamma(R) \)**

Let \( R_0 \) denote the set \{ \( aE_{11} + bE_{12} + cE_{21} + dE_{22} \mid a - d \in U(\mathbb{Z}_p') \) or \( b \in U(\mathbb{Z}_p') \) or \( c \in U(\mathbb{Z}_p') \) \}. Then \( R \setminus R_0 = \{ aE_{11} + bE_{12} + cE_{21} + dE_{22} \mid a - d \in D(\mathbb{Z}_p'), b \in D(\mathbb{Z}_p') \) and \( c \in D(\mathbb{Z}_p') \} \). Since \( |D(\mathbb{Z}_p')| = p^{|x|-1} \), an easy computation shows that \( |R \setminus R_0| = p^{4|x|-3} \). Therefore \( |R_0| = p^{4|x| - p^{4|x|-3}} \). For \( A, B \in R \), we write \( A \sim B \) if there exist \( a \in U(\mathbb{Z}_p') \) and \( b \in \mathbb{Z}_p \), such that \( A = aB + bE \). A trivial verification shows that \( \sim \) is an equivalence relation on \( R \). Set \( [A] = \{ B \in R \mid A \sim B \} \). It follows immediately that \( [A] \) is the equivalence class of \( A \) on \( R \) under the equivalence relation of \( \sim \).

**Lemma 3.1.** Every equivalence class in \( R_0 \) has size \( p^{2|x|} - p^{2|x|-1} \). Moreover, there are \( p^{2|x|} + p^{2|x|-1} + p^{2|x|-2} \) distinct equivalence classes in \( R_0 \).

**Proof.** Assume that \( A = aE_{11} + bE_{12} + cE_{21} + dE_{22} \in R_0 \), where \( a - d \in U(\mathbb{Z}_p') \) or \( b \in U(\mathbb{Z}_p') \) or \( c \in U(\mathbb{Z}_p') \). Let \( A_1 = a_1A_1 + b_1E \) and \( A_2 = a_2A_2 + b_2E \in [A] \), where \( a_1, a_2 \in U(\mathbb{Z}_p') \) and \( b_1, b_2 \in \mathbb{Z}_p \). We claim that if \( a_1 \neq a_2 \) or \( b_1 \neq b_2 \), then \( A_1 \neq A_2 \). If \( a_1 = a_2 \) and \( b_1 = b_2 \), then \( A_1 - A_2 = (b_1 - b_2)E \). It is clear that \( A_1 \neq A_2 \). If \( a_1 \neq a_2 \) and \( b_1 = b_2 \), then \( A_1 - A_2 = ((a_1 - a_2)(a - d) + (a_1 - a_2)d)E_{11} + (a_1 - a_2)bE_{12} + (a_1 - a_2)cE_{21} + (a_1 - a_2)dE_{22} \). If \( (a_1 - a_2)d \neq 0 \), then \( (a_1 - a_2)(a - d) + (a_1 - a_2)d \neq 0 \) or \( (a_1 - a_2)c \neq 0 \) (i.e., \( A_1 \neq A_2 \)), since \( a_1 - a_2 \neq 0, a - d \in U(\mathbb{Z}_p') \) or \( b \in U(\mathbb{Z}_p') \) or \( c \in U(\mathbb{Z}_p') \). If \( (a_1 - a_2)d = 0 \), then it is obvious that \( A_1 \neq A_2 \). If \( a_1 \neq a_2 \) and \( b_1 \neq b_2 \), then \( A_1 - A_2 = ((a_1 - a_2)(a - d) + (a_1 - a_2)d + b_1 - b_2)E_{11} + (a_1 - a_2)bE_{12} + (a_1 - a_2)cE_{21} + (a_1 - a_2)d + b_1 - b_2)E_{22} \). Similarly, we have \( A_1 \neq A_2 \). It is well known that \( |U(\mathbb{Z}_p')| = p^{|x| - p^{-1}} \). So \( ||A|| = p^{2|x|} - p^{2|x|-1} \).

It is easily seen that if \( A \in R_0 \), then \( [A] \subseteq R_0 \). This fact makes it obvious that \( R_0 \) is the disjoint union of some equivalence classes. Since \( |R_0| = p^{3|x|} - p^{4|x|-3} \), there are exactly \( p^{2|x|} + p^{2|x|-1} + p^{2|x|-2} \) equivalence classes in \( R_0 \).
In fact, a trivial verification shows that the set of equivalence class representatives in $R_0$ is
\[\{E_{11} + aE_{12} + bE_{21}, \ aE_{11} + E_{12} + bE_{21}, \ aE_{11} + bE_{12} + E_{21},\]
\[E_{11} + cE_{12} + bE_{21}, \ E_{11} + bE_{12} + cE_{21}, \ bE_{11} + E_{12} + cE_{21},\]
\[E_{11} + cE_{12} + dE_{21} \mid a, b \in \langle p \rangle, \ c, d \in U(\mathbb{Z}_{p^r}).\]

We denote this set by $P_0$. By Lemma 3.1, we can write
\[P_0 = \{A_{0,1}, A_{0,2}, \cdots, A_{0,p^r+p^{2r-1}+p^{2r-2}}\}.\]

It is immediate that $R_0 = \bigcup_{i=0}^{\lfloor s/2 \rfloor} \{A_{0,i}\}$. Let $j \in \{1, 2, \cdots, s - 1\}$. Set $P_j = p^j P_0$. Since $\mathbb{Z}_{p^r}$ is a principal ideal ring,
\[P_j = \{p^j E_{11} + aE_{12} + bE_{21}, \ aE_{11} + p^j E_{12} + bE_{21}, \ aE_{11} + bE_{12} + p^j E_{21},\]
\[p^j E_{11} + cE_{12} + bE_{21}, \ p^j E_{11} + bE_{12} + cE_{21}, \ bE_{11} + p^j E_{12} + cE_{21},\]
\[p^j E_{11} + cE_{12} + dE_{21} \mid a, b \in \langle p^j \rangle, \ c, d \in \text{Ass}(p^j)\].

From Lemma 3.1, $|P_j| = p^{2s-2j} + p^{2s-2j-1} + p^{2s-2j-2}$. Write $P_j = \{A_{j,1}, A_{j,2}, \cdots, A_{j,|P_j|}\}$. Set
\[R_j = \bigcup_{i=j}^{\lfloor s/2 \rfloor} \{A_{j,i}\}. \tag{3.1}\]

Accordingly, there are seven forms in $\bigcup_{j=0}^{s-1} P_j$. For example, let $j, k \in \{0, 1, \cdots, s - 1\}$, if $A_{j,j} = p^j E_{11} + a_1 E_{12} + b_1 E_{21}, A_{k,k} = a_2 E_{11} + p^k E_{12} + b_2 E_{21}$, where $a_1, b_1 \in \langle p^j \rangle, a_2, b_2 \in \langle p^k \rangle$, then we say that $A_{j,j}$ and $A_{k,k}$ have different forms.

**Lemma 3.2.** Let $R_j = \bigcup_{i=j}^{\lfloor s/2 \rfloor} \{A_{j,i}\}$, where $j = 0, 1, \ldots, s - 1$. Then
\[R = \bigcup_{j=0}^{s-1} R_j \bigcup C(R) = \bigcup_{j=0}^{s-1} \{A_{j,i}\} \bigcup C(R)\]
is a partition of $R$.

**Proof.** By the definition of $C(R)$, we have $C(R) \cap R_j = \emptyset$ for all $j \in \{0, 1, \cdots, s - 1\}$. By construction, $C(R) \not\subseteq R_0$ and hence $C(R) \not\subseteq R_j$ for $j \in \{1, 2, \cdots, s - 1\}$. Let $A_{j,j} \in P_j$. Then $A_{j,j} = p^j A_{0,0}$ for a certain $A_{0,0} \in P_0$. Consequently, $[A_{j,j}] = [p^j A_{0,0}] = \{a p^j A_{0,0} + bE \mid a \in U(\mathbb{Z}_{p^r}) \text{ and } b \in \mathbb{Z}_{p^r}\} = \{a A_{0,0} + bE \mid a \in \text{Ass}(p^j) \text{ and } b \in \mathbb{Z}_{p^r}\}$. By Lemma 2.1, in the same way as Lemma 3.1, the size of an equivalence class in $R_j$ is $p^{2s-j} - p^{2s-j-1}$. It follows that $|R_j| = p^{4s-j} - p^{4s-j-3}$. Then
\[\sum_{j=0}^{s-1} |R_j| + |C(R)| = \sum_{j=0}^{s-1} (p^{4s-j} - p^{4s-j-3}) + p^s = p^{4s} = |R|.

It remains to prove that $R_{j_1} \cap R_{j_2} = \emptyset$ for all $j_1 \neq j_2 \in \{0, 1, \cdots, s - 1\}$. Assume that $A \in R_{j_1} \cap R_{j_2} \neq \emptyset$. There exist $a_1, a_2 \in U(\mathbb{Z}_{p^r}), b_1, b_2 \in \mathbb{Z}_{p^r}$, $A_{j_1,j_1} \in P_{j_1}$ and $A_{j_2,j_2} \in P_{j_2}$ such that $A = a_1 A_{j_1,j_1} + b_1 E = a_2 A_{j_2,j_2} + b_2 E$. It implies that $A_{j_1,j_1} = a_1^{-1} a_2 A_{j_2,j_2} + a_1^{-1}(b_2 - b_1)E$. Since the (2, 2) entries of $A_{j_1,j_1}$ and $A_{j_2,j_2}$ are equal to 0, $a_1^{-1}(b_2 - b_1) = 0$. Thus, $A_{j_1,j_1} = a_1^{-1} a_2 A_{j_2,j_2}$. Suppose that $A_{j_1,j_1} = p^{j_1} E_{11} + \cdots + p^{j_1} E_{12} + \cdots + E_{21}$ and $A_{j_2,j_2} = p^{j_2} E_{11} + \cdots + p^{j_2} E_{12} + \cdots + E_{21}$. We thus get $j_1 = j_2$. This contradicts our assumption $j_1 \neq j_2$. Similarly, we obtain contradictions in the other cases of $A_{j_1,j_1}$ and $A_{j_2,j_2}$. This completes the proof. \(\square\)
Lemma 3.3. Let $A \in \{A_{j|i}\}$, $B \in \{A_{k|i}\}$, where $j, k \in \{0, 1, \ldots, s - 1\}$, $A_{j|i} \in P_j$ and $A_{k|i} \in P_k$.

(i) Let $j + k \leq s - 1$. Then $AB = BA$ if and only if $p^iA_{j|i} = p^iA_{k|i}$.

(ii) Let $j + k > s - 1$. Then $AB = BA$.

Proof. It is easily seen that $AB = BA$ if and only if $A_{j|i}A_{k|i} = A_{k|i}A_{j|i}$.

(i) Suppose that $A_{j|i} = p^iE_{11} + a_1E_{12} + b_1E_{21}$, $A_{k|i} = p^kE_{11} + a_2E_{12} + b_2E_{21}$, where $a_1, b_1 \in \langle p^{j+1} \rangle$, $a_2, b_2 \in \langle p^{k+1} \rangle$. Then $A_{j|i}A_{k|i} = \star E_{11} + \star p^{j+k}E_{12} + \star E_{21}$, $A_{k|i}A_{j|i} = \star E_{11} + \star p^{j+k+2}E_{12} + \star E_{21}$. Obviously, $A_{j|i}A_{k|i} \neq A_{k|i}A_{j|i}$. By similar arguments, it is easy to check that $A_{j|i}A_{k|i} \neq A_{k|i}A_{j|i}$ when $A_{j|i}$ and $A_{k|i}$ have different forms.

Without loss of generality we assume that $j \geq k$. Now suppose that $A_{j|i}A_{k|i} = A_{k|i}A_{j|i}$, where $A_{j|i} = p^iE_{11} + a_1E_{12} + b_1E_{21}$, $A_{k|i} = p^kE_{11} + a_2E_{12} + b_2E_{21}$, $a_1, b_1 \in \langle p^{j+1} \rangle$, $a_2, b_2 \in \langle p^{k+1} \rangle$. By Lemma 2.1, we can assume that $a_1 = \sum_{i=j+1}^{s-1} r_ip^i$, $b_1 = \sum_{i=j+1}^{s-1} t_ip^i$, $a_2 = \sum_{i=k+1}^{s-1} u_ip^i$ and $b_2 = \sum_{i=k+1}^{s-1} v_ip^i$, where $r_i, t_i, u_i, v_i \in T$. Since $A_{j|i}A_{k|i} = A_{k|i}A_{j|i}$, it is obvious that $r_j = u_{k+1}, r_{j+2} = u_{k+2}, \ldots, r_{s-k-1} = u_{s-j-1}, t_{j+1} = v_{k+1}, t_{j+2} = v_{k+2}, \ldots, t_{s-k-1} = v_{s-j-1}$. It is immediately that $p^kA_{j|i} = p^kA_{k|i}$. In other cases we conclude similarly that $p^kA_{j|i} = p^kA_{k|i}$.

Conversely, suppose that $p^kA_{j|i} = p^kA_{k|i}$. An easy computation shows that it occurs only when $A_{j|i}$ and $A_{k|i}$ have same form. Assume that $A_{j|i} = p^iE_{11} + a_1E_{12} + b_1E_{21}$, $A_{k|i} = p^kE_{11} + a_2E_{12} + b_2E_{21}$ with $a_1 = \sum_{i=j+1}^{s-1} r_ip^i$, $b_1 = \sum_{i=j+1}^{s-1} t_ip^i$, $a_2 = \sum_{i=k+1}^{s-1} u_ip^i$ and $b_2 = \sum_{i=k+1}^{s-1} v_ip^i$, where $r_i, t_i, u_i, v_i \in T$. Since $p^kA_{j|i} = p^kA_{k|i}$, it is easy to check that $r_{j+1} = u_{k+1}, r_{j+2} = u_{k+2}, \ldots, r_{s-k-1} = u_{s-j-1}, t_{j+1} = v_{k+1}, t_{j+2} = v_{k+2}, \ldots, t_{s-k-1} = v_{s-j-1}$. It is clear that $A_{j|i}A_{k|i} = A_{k|i}A_{j|i}$. The proof for other cases is similar.

(ii) If $j + k > s - 1$, then $A_{j|i}A_{k|i} = 0 = A_{k|i}A_{j|i}$. Therefore, $AB = BA$. \hfill \Box

For fixed $j, k \in \{0, 1, \ldots, s - 1\}$ and $i_k \in \{1, 2, \ldots, |P_k|\}$, set

$$R_{j, k} = \{[A_{j|i}] \subseteq R_j \mid p^iA_{j|i} = p^iA_{k|i}\}.$$ 

By Lemma 3.3, we have the following proposition.

Proposition 3.4. Let $A \in \{A_{k|i}\}$, where $k \in \{0, 1, \ldots, s - 1\}$ and $A_{k|i} \in P_k$.

(i) $C_R(A) = \bigcup_{j=0}^{s-1} \{p^iA_{0|i}\} \cup C(R)$.

(ii) Let $0 < j \leq s - 1$. Then $C_R(A) = \bigcup_{j=0}^{s-k-1} R_{j, k} \bigcup_{j=s-k}^{s-1} R_j \bigcup C(R)$.

For fixed $k, j \in \{0, 1, \ldots, s - 1\}$, $k \geq j$, $i_k \in \{1, 2, \ldots, |P_k|\}$, $i_{k+1} \in \{1, 2, \ldots, |P_{k+1}|\}$, $\ldots, i_{s-1} \in \{1, 2, \ldots, |P_{s-1}|\}$, if $p^{s-1-k}A_{j+i_{k+1}} = p^{s-1-(k+1)}A_{k+i_{k+1}} = \cdots = p^0A_{s-1,i_{s-1}}$, then set

$$R_{j,i_{k+1},\ldots,i_{s-1}} = \{[A_{j|i}] \subseteq R_j \mid p^iA_{j+i_{k+1}} = A_{k+i_{k+1}}\},$$

$$N_{j+k}^i = \{i_{k-1} \in \{1, \ldots, |P_k|\} \mid p^iA_{k+i_{k-1}} = A_{k+i_{k-1}}\}.$$ 

Since $p^{s-1-j}P_j = p^{s-1-(j+1)}P_{j+1} = \cdots = P_{s-1}$,

$$R_j = \bigcup_{i_{j+1}=1}^{P_{j+1}} R_{j,i_{j+1}} = \cdots = \bigcup_{i_{j+1} \in N_{j+1}^j} \bigcup_{i_{j+2} \in N_{j+2}^{j+1}} \cdots \bigcup_{i_{s-1}=1} P_{s-1} R_{j,i_{s-1},\ldots,i_{s-1}}.$$
Lemma 3.5. Let 0 ≤ j ≤ k ≤ s − 1, A_{k,j} ∈ P_k, A_{k+1,j+1} ∈ P_{k+1}, · · · , A_{s−1,s−1} ∈ P_s and \( p^{s−1−(k−1)}A_{k,j} = p^{s−1−(k+1)}A_{k+1,j+1} = · · · = p^0A_{s−1,s−1} \). Then the number of equivalence classes in \( R_{j_1, · · · , j_{s−1},i_k} \) is \( p^{2(k−j)} \).

Proof. From the construction of \( P_j \) and \( P_k \), we know that \( p^{k−j}P_j = p^kP_0 = P_k \). Define two maps \( f : \langle p^{k+1} \rangle \to \langle p^{k+1} \rangle \) by \( \Sigma_{i=0}^{s−1} t_ip^i \mapsto \Sigma_{i=0}^{s−1} t_ip^{s−1−j} \) and \( g : \text{Ass}(p^i) \to \text{Ass}(p^k) \) by \( \Sigma_{i=0}^{s−1} t_ip^i \mapsto \Sigma_{i=0}^{s−1} t_ip^{s−1−j} \), where \( t_j \in T^* \), \( t_i \in T \), \( i = j + 1, j + 2, · · · , s \). Clearly, \( f \), \( g \) are surjective, and we have \( \ker(f) = \{ \Sigma_{i=0}^{s−1} t_ip^i \mid t_i \in T \}, i = s − k + j, s − k + j + 1, · · · , s − 1 \} = \langle p^{s−1−j} \rangle \) and \( \ker(g) = \{ p^i + \Sigma_{i=0}^{s−1−j} t_ip^i \mid t_i \in T \}, i = s − k + j, s − k + j + 1, · · · , s − 1 \}. By Lemma 2.1 and \( |T| = p \), \( |\ker(f)| = |\ker(g)| = p^{k−j} \). Then the size of the inverse image of each element in \( \langle p^{k+1} \rangle \) and \( \text{Ass}(p^k) \) under \( f \) and \( g \) is \( p^{k−j} \). Moreover, it is evident that the number of solutions of \( p^{k−j}X = A_{k,i} \) in \( P_j \) is \( p^{2(k−j)} \). In fact, the number of equivalence classes in \( R_{j_1, · · · , j_{s−1},i_k} \) is equal to the number of solutions of \( p^{k−j}X = A_{k,i} \) in \( P_j \), which completes the proof.

From Lemma 3.5, \( |N_{k−1}^{i_k}| = p^2 \) for all \( k \in \{1, 2, · · · , s−1\} \) and \( i_k \in \{1, 2, · · · , |P_k|\} \). Recall that \( \Omega_{p^2} = \{1, 2, · · · , p^2\} \). It is easily seen that there exists a unique map \( \varphi_{i_k} : N_{k−1}^{i_k} \to \Omega_{p^2} \) such that for \( i, j \in N_{k−1}^{i_k} \), if \( i < j \), then \( \varphi_{i_k}(i) < \varphi_{i_k}(j) \). Let \( i_k \in \{1, 2, · · · , |P_k|\} \). Define a map

\[
\varphi_{k−1}^{i_k} : N_{k−1} \to N_{k−1}^{i_k}
\]

by \( i \mapsto j \) if \( \varphi_{i_k}(i) = \varphi_{i_k}(j) \).

Corollary 3.6. Let \( R = M_2(\mathbb{Z}_{p^2}) \), with \( p \) prime and \( s \) positive integer. Let \( A, B \in R \). Then \( C_R(A) = C_R(B) \) if and only if \( \{A = B\} \).

Proof. If \( A, B \in C(R) \), it is obviously that \( C_R(A) = R = C_R(B) \) if and only if \( \{A = B\} \). If \( A \in C(R) \) and \( B \notin C(R) \), it is clear that \( C_R(A) = R \neq C_R(B) \). Similarly, if \( A \notin C(R) \) and \( B \in C(R) \), then \( C_R(A) \neq C_R(B) \).

Now let \( A, B \in R \setminus C(R) \). Suppose that \( C_R(A) = C_R(B) \), where \( A \in \{A_{j,i}\}, B \in \{A_{k,\bar{i}}\}, j, k \in \{0, 1, · · · , s−1\} \). We claim that \( j = k \) and \( i_j = i_k \). If \( j = 0 \) and \( k \neq 0 \), by Proposition 3.4, we know that \( C_R(A) \neq C_R(B) \), a contradiction. Similarly, if \( j \neq 0 \) and \( k = 0 \), then \( C_R(A) \neq C_R(B) \), a contradiction. If \( 0 < j < k \leqslant s−1 \), then \( \bigcup_{i=j}^{s−1} R_i \neq \bigcup_{i=j}^{s−1} R_i \). By Proposition 3.4 (ii), \( C_R(A) = \bigcup_{i=0}^{s−1−j} R_i^{i,j} \bigcup_{i=s−k}^{s−1} R_i \neq \bigcup_{i=0}^{s−1} R_i^{i,j} \bigcup_{i=s−k}^{s−1} R_i = C_R(B) \), a contradiction. If \( j = k = 0 \) and \( i_j \neq i_k \), then \( \{A_{0,i_j}\} \neq \{A_{0,i_k}\} \). By Proposition 3.4 (i), \( C_R(A) = \bigcup_{i=0}^{s−1} [p^iA_{0,i_j}] \neq \bigcup_{i=0}^{s−1} [p^iA_{0,i_k}] = C_R(B) \), a contradiction. If \( 0 < j = k \leqslant s−1 \) and \( i_j \neq i_k \), then \( A_{j,i_j} \neq A_{j,k} \). Thus, by the proof of Lemma 3.5, \( R_0^{i,j} = R_0^{i,k} \). Furthermore, \( C_R(A) = R_0^{i,j} \bigcup_{i=0}^{s−1−j} R_i^{i,j} \bigcup_{i=s−j}^{s−1} R_i \neq R_0^{i,k} \bigcup_{i=0}^{s−1−j} R_i^{i,k} \bigcup_{i=s−j}^{s−1} R_i = C_R(B) \) by Proposition 3.4 (ii), a contradiction. Therefore \( j = k \) and \( i_j = i_k \) as claimed. This means that \( A_{j,i} = A_{k,i} \) (i.e. \( \{A = B\} \)). The converse is straightforward.

Corollary 3.7. Let \( R = M_2(\mathbb{Z}_{p^2}) \), with \( p \) prime and \( s \) positive integer. If \( f \in \text{Aut}(\Gamma(R)) \), then \( f(R_j) = R_j \) for \( j \in \{0, 1, · · · , s−1\} \), where \( R_j \) is as defined in (3.1).

Proof. For \( j = 0, 1, · · · , s−1 \), if \( A \in R_j \), then \( |C_R(A) \setminus C(R)| = p^{2s−2} = p^2 \) by Proposition 3.4 and the proof of Lemma 3.5. This means that if \( A \in R_j \), \( B \in R_j \) and \( j \neq k \), then \( |N(A)| \neq |N(B)| \), where \( j, k \in \{0, 1, · · · , s−1\} \). Since automorphisms of a graph must preserve the number of neighbors of vertices, \( f(R_j) = R_j \), where \( j \in \{0, 1, · · · , s−1\} \).
Recall that a graph automorphism of a graph $G$ is a bijection on vertex set which preserves adjacency. If $|V(G)| = n$, then in the obvious way $\text{Aut}(G)$ is isomorphic to a subgroup of $S_n$. Specifically, $\text{Aut}(G) = \{ f \in S_n \mid \text{for all } x, y \in V(G), [x, y] \Rightarrow [f(x), f(y)] \}$. It is easy to show that $\text{Aut}(G) = \{ f \in S_n \mid \text{for all } x \in V(G), f(N(x)) = N(f(x)) \}$. For $\Gamma(R)$, $N(A) = C_R(A) \setminus \{C(R) \cup A\}$. This means that $\text{Aut}(\Gamma(R)) = \{ f \in S_{\sum_{p \mid |R_j|} |f|} \mid \text{for all } A \in V(\Gamma(R)), f(N(A)) = N(f(A)) \}$.

We now prove our main result about the automorphism group of the commuting graph of $M_2(\mathbb{Z}_p)$. To state it, we need to define a group. For each $j \in \{0, 1, \ldots, s - 1\}$ denote

$$G_{s-1-j} = S_{p^{2s-1-j-1}} \times \cdots \times S_{p^{2s-1-j-1}} \times S_{p^{2s+1}}.$$

Let $G$ be a subset of $\prod_{j=0}^{s-1} G_{s-1-j}$ and define:

$$G = \{ (h_0 \times g_0 \times \cdots \times g_{s-2} \times h_1 \times g_1 \times \cdots \times g_{s-1}, \cdots, h_{s-1} \times g_{s-1}) \mid h_j \times g_j \times \cdots \times g_{s-2} \times g_{s-1} \in G_{s-1-j}, \; j = 0, 1, \ldots, s-1 \}. \quad (3.3)$$

The multiplication law of the iterated wreath product is defined in [11, p. 68], the proof that $G$ is a subgroup of $\prod_{j=0}^{s-1} G_{s-1-j}$ is routine.

**Theorem 3.8.** Let $R = M_2(\mathbb{Z}_p)$, with $p$ prime and $s$ positive integer. Then $\text{Aut}(\Gamma(R)) \cong G$, where $G$ is a group defined in (3.3).

**Proof.** By Lemma 3.2 and Corollary 3.7, $\text{Aut}(\Gamma(R))$ is isomorphic to a subgroup of $\prod_{j=0}^{s-1} S_{R_j}$. So $f \in \text{Aut}(\Gamma(R))$ can be written as a product $\prod_{j=0}^{s-1} f_j$, where $f_j \in S_{R_j}$. We claim that

$$\{ f_j \in S_{R_j} \mid (\cdots, f_j, \cdots) = f \in \text{Aut}(\Gamma(R)) \} \cong G_{s-1-j},$$

where $j = 0, 1, \ldots, s-1$.

Let $j \in \{1, \ldots, s-1\}$ and $(\cdots, f_j, \cdots) = f \in \text{Aut}(\Gamma(R))$. Assume that $A \in [A_{s-1-j}, \; B \in [A_{s-1-j}]$ with $f_j(A) = B$. By Proposition 3.4 (ii) and $f(N(A)) = N(f(A))$,

$$f(R^j_0^{s-j-1} \bigcup R^j_1^{s-j-1} \bigcup R_k) = R^j_0^{s-j-1} \bigcup R^j_1^{s-j-1} \bigcup R_k.$$

Then $f(R^j_0^{s-j-1}) = R^j_0^{s-j-1}$ by Corollary 3.7. It is immediate that $f([A_{s-1-j}, \; A_{s-1-j}]) = [A_{s-1-j}, \; A_{s-1-j}]$ by Proposition 3.4 (i), where $[A_{s-1-j}, \; A_{s-1-j}] = p^{s-1}R^j_0^{s-j-1} = p^{s-1}R^j_0^{s-j-1}$. Since Proposition 3.4 (ii) and $f(N([A_{s-1-j}, \; A_{s-1-j}])) = N(f([A_{s-1-j}, \; A_{s-1-j}]))$,

$$f(R^j_0^{s-1-j} \bigcup R_k) = R^j_0^{s-1-j} \bigcup R_k.$$ 

Thus $f(R^j_0^{s-1-j}) = R^j_0^{s-1-j}$. It is evident that $f(p^j R^j_0^{s-1-j}) = p^j R^j_0^{s-1-j}$ by Proposition 3.4 (i), i.e.,

$$f_j(R^j_0^{s-1-j}) = R^j_0^{s-1-j}.$$
Similarly, we have
\[ f_j(R_{i\delta i+1, s-2}) = R_{i\delta i+1, s-2}, \]
\[ \ldots \]
\[ f_j(R_{i\delta i+1, s-2, j+1}) = R_{i\delta i+1, s-2, j+1}, \]
where \( i_{s-2}, i'_{s-2} \in \{1, \ldots, |P_{s-2}|\}, \ldots, i_{j+1}, i'_{j+1} \in \{1, \ldots, |P_{j+1}|\} \) with
\[ A_{i_{s-2}, i_{s-2}} = p^{s-2-j} A_{i_{s-2}} A_{i_{s-2}, i_{s-2}} = p^{s-2-j} A_{i_{s-2}} \]
\[ \ldots \]
\[ A_{i_{j+1}, i_{j+1}} = p A_{i_{j+1}} A_{i_{j+1}, i_{j+1}} = p A_{i_{j+1}}. \]

Obviously,
\[ f_j(R_{i\delta i+1, s-2, \ldots, j+1}) = f_j([A_{i\delta j}]) = [A_{i\delta j}] = R_{i\delta i+1, \ldots, j+1}. \]

Hence, for \( i_{s-1} \in \{1, 2, \ldots, |P_{s-1}|\}, i_{s-2} \in N_{s-2}^{j_{s-2}}, \ldots, i_{j+1} \in N_{j+1}^{j_{j+1}}, i_j \in N_j^{j_{j+1}}, \) there are \( i'_{s-1} \in \{1, 2, \ldots, |P_{s-1}|\}, i'_{s-2} \in N_{s-2}^{j_{s-2}}, \ldots, i'_{j+1} \in N_{j+1}^{j_{j+1}}, i'_j \in N_j^{j_{j+1}} \) such that
\[ f_j(R_{i\delta i+1}) = R_{i'\delta i+1}, \]
\[ f_j(R_{i\delta i+1, i_{s-2}}) = R_{i'\delta i+1, i'_{s-2}}, \]
\[ \ldots \]
\[ f_j(R_{i\delta i+1, \ldots, j+1}) = R_{i'\delta i+1, \ldots, j+1}. \]

By Lemma 3.5, \( |N_k^{j_{s-1}}| = p^2, k = j, j + 1, \ldots, s - 2. \) In the proof of Lemma 3.2, we know that \( ||A|| = p^{2s-j} - p^{2s-j-1} \) for \( A \in R_j. \) Therefore \( \{f_j \in S_{R_j} | (\ldots, f_j, \ldots) = f \in \text{Aut}(\Gamma(R))\} \cong G_{s-1-j} \) by Corollaries 2.4 and 3.6. The proof for \( j = 0 \) is similar.

From the above proof, it follows that \( \text{Aut}(\Gamma(R)) \) is a subgroup of \( \prod_{j=0}^{s-1} G_{s-1-j}. \) Let \( j \in \{0, 1, \ldots, s-2\}. \) Let \( \phi_j \) be an isomorphism between \( \{f_j \in S_{R_j} | (\ldots, f_j, \ldots) = f \in \text{Aut}(\Gamma(R))\} \) and \( G_{s-1-j}. \) Suppose that \( (\ldots, f_j, f_{j+1}, \ldots) = f \in \text{Aut}(\Gamma(R)), \) where \( \phi_j(f_j) = h_j \mapsto g_j \mapsto \ldots \mapsto g_{s-2} \mapsto g_{s-1} \in G_{s-1-j}. \) As defined in (2.1), \( g_{s-1} \in S_{p^2+j+1}, \)
\[ g_k = \prod_{i_{s-1} \in N_{i_{s-1}}^{j_{s-1}}} \prod_{i_{s-2} \in N_{i_{s-2}}^{j_{s-2}}} \cdots \prod_{i_{j+1} \in N_{i_{j+1}}^{j_{j+1}}} \prod_{i_{s-2} \in N_{i_{s-2}}^{j_{s-2}}} \cdots \prod_{i_{s-1} = 1}^{p^2+j+1} S_{A_{i_{s-1}}}, \]
\[ k = s-2, s-3, \ldots, j, \] and
\[ h_j = \prod_{i_{j+1} \in N_{i_{j+1}}^{j_{j+1}}} \prod_{i_{j+1} \in N_{i_{j+1}}^{j_{j+1}}} \cdots \prod_{i_{j+1} \in N_{i_{j+1}}^{j_{j+1}}} \prod_{i_{j+1} \in N_{i_{j+1}}^{j_{j+1}}} \cdots \prod_{i_{j+1} = 1}^{p^2+j+1} S_{A_{i_{j+1}}}. \]

As the action defined in (2.2), we define \( f_j(R_{i\delta i+1}) = R_{i\delta i+1}, \)
\[ f_j(R_{i\delta i+1, \ldots, j+1}) = R_{i\delta i+1, \ldots, j+1}. \]
where $y_{s-1} = g_{s-1}(i_{s-1})$, $y_k = g_{k,y_{s-1} \cdots y_{k+2}, y_{k+1}}(\varphi_k^{y_{k+1}}(i_k))$, $\varphi_k^{y_{k+1}}$ is defined in (3.2), $k = s - 2, s - 3, \ldots, j$ and $f_j(aA_{ij} + bE) = h_{j,y_{s-1} \cdots y_{j+1}}(aA_{ij} + bE)$ for all $a \in \text{Ass}(p^l)$, $b \in \mathbb{Z}_{p^l}$. Suppose that $\phi_{j+1}(f_{j+1}) = h_{j+1} \wr g_{j+1} \wr \cdots \wr g_{s-2} \wr g_{s-1} \in G_{s-1} \wr (j+1)$. We next claim that $g_{j+1} = g_{j+1}', g_{j+2} = g_{j+2}', \ldots, g_{s-1} = g_{s-1}'. If there exists $k \in \{j+1, j+2, \ldots, s-1\}$ such that $g_{j+1} = g_{j+1}', g_{k-1} = g_{k-1}', g_k \neq g_k'$, $g_{k+1} = g_{k+1}', \ldots, g_{s-1} = g_{s-1}'$, then there exist $i_{s-1} \in \{1, 2, \ldots, p^2 + p + 1\}, \ldots, i_{k+1} \in N_{k+2}^{k+2}, i_k \in N_{k+1}^{k+1}$ such that $y_k \neq y_k'$, where $y_k, y_k'$ are defined above. Assume that $f_j(R_{j,y_{s-1} \cdots y_{j+1}, y_{j+1}}) = R_{j,y_{s-1} \cdots y_{k+1}, y_{k+1}}$ and $f_{j+1}(R_{j+1,y_{s-1} \cdots y_{k+1}, y_{k+1}}) = R_{j+1,y_{s-1} \cdots y_{k+1}, y_{k+1}}'. By Proposition 3.4 (i) and $f(N(A)) = f(N(A))$ for all $A \in R \setminus C(R)$, $f_0(R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}) = R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}$ and $f_0(R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}) = R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}'. Since $y_k \neq y_k'$, $R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}} \neq R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}'$, i.e., $f_0(R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}}) \neq f_0(R_{0,y_{s-1} \cdots y_{k+1}, y_{k+1}})$, which is impossible. By this claim, we know that $f \in \text{Aut}(\Gamma(R))$ can be written as $(h_0 \wr g_0 \wr \cdots \wr g_{s-2} \wr g_{s-1}, h_1 \wr g_1 \wr \cdots \wr g_{s-2} \wr g_{s-1}, \ldots, h_{s-1} \wr g_{s-1})$, where $h_j \wr g_j \wr \cdots \wr g_{s-2} \wr g_{s-1} \in G_{s-1-j}, j = 0, 1, \ldots, s-1. Therefore \text{Aut}(\Gamma(R)) \cong G. □$

4. Conclusions

In this paper, we show that the automorphism group of $\Gamma(M_2(\mathbb{Z}_{p^l}))$ is a subgroup of a direct product of some wreath products, and we completely characterize it in Theorem 3.8.

Acknowledgments

The author wishes to express his thanks to the referees for their time and comments.

Conflict of interest

The author declares no conflicts of interest in this paper.

References