International Electronic Journal of Algebra
Volume 22 (2017) 147-169
DOI: 10.24330/ieja.325941

IDEMPOTENTS AND UNITS OF MATRIX RINGS OVER POLYNOMIAL RINGS

Pramod Kanwar, Meenu Khatkar and R. K. Sharma

Received: 15 January 2017; Revised: 16 February 2017
Communicated by Surrender K. Jain

Abstract. The aim of this paper is to study idempotents and units in certain matrix rings over polynomial rings. More precisely, the conditions under which an element in $M_2(\mathbb{Z}_p[x])$ for any prime p, an element in $M_2(\mathbb{Z}_{2p}[x])$ for any odd prime p, and an element in $M_2(\mathbb{Z}_{3p}[x])$ for any prime p greater than 3 is an idempotent are obtained and these conditions are used to give the form of idempotents in these matrix rings. The form of elements in $M_2(\mathbb{Z}_2[x])$ and elements in $M_2(\mathbb{Z}_3[x])$ that are units is also given. It is observed that unit group of these rings behave differently from the unit groups of $M_2(\mathbb{Z}_2)$ and $M_2(\mathbb{Z}_3)$.

Mathematics Subject Classification (2010): 16S50, 13F20, 16U60
Keywords: Idempotent, unit, polynomial ring, matrix ring

1. Introduction

Idempotents and units in rings play a critical role in the study of rings. Several classes of elements are defined using idempotents and units, for example, clean elements (the elements that can be expressed as a sum of an idempotent and a unit, cf. [8], [13]), strongly clean elements (the elements that can be expressed as a sum of an idempotent and a unit that commute, cf. [14]), unit regular elements (the elements that can be written as eu for some idempotent e and unit u, cf. [6], [14]), Lie regular elements (the elements that can be written as $eu - ue$ where e is an idempotent and u is a unit, cf. [15]), etc. Due to their importance, the idempotents and units generated interest among several researchers and efforts have been made to compute idempotents and unit groups of rings.

The problem of obtaining structure and presentation of unit groups of rings have also drawn attention of several researchers. Important contributions have been made in some special cases (for example see [1], [2], [3], [5], [9], [10], [12], [15], [16]). These studies, however, are far from complete and a lot more needs to be done. In the case of polynomial rings, Kanwar, Leroy and Matczuk showed that for an abelian ring (a ring in which all idempotents are central) R, idempotents

in the polynomial ring $R[x]$ over R are precisely idempotents in R ([7, Lemma 1]) and that for a reduced ring R, the units in the polynomial ring $R[x]$ over R are precisely the units in R ([8, Corollary 1.7]). In fact, a ring R is reduced if and only if the unit group of $R[x]$ is same as the unit group of R. Not much, however, is known in the case of polynomial rings over matrix rings (equivalently, matrix rings over polynomial rings).

In this article, we study idempotents and units in certain matrix rings over polynomial rings. We give conditions for elements in $M_2(\mathbb{Z}_{2p}[x])$ (where p is an odd prime) and $M_2(\mathbb{Z}_{3p}[x])$ (where p is a prime greater than 3) to be idempotent and use these to give form of idempotents in these rings (Theorems 3.5 and 3.7). We also show that for any ring R, every derived subgroup of the unit group of the matrix ring of $n \times n$ matrices over the polynomial ring $R[x]$ has units of certain form that are commutators of units of the same form (Proposition 4.1 and Corollary 4.2) showing, as a byproduct, that the unit group of $M_n(R[x])$ is not solvable. In Theorem 4.4 and Theorem 4.5, we give conditions for elements of $M_2(\mathbb{Z}_2[x])$ and $M_2(\mathbb{Z}_3[x])$ to be units and use these to give form of units in these rings. We further observe that unit group of $M_2(\mathbb{Z}_2[x])$ and unit group of $M_2(\mathbb{Z}_3[x])$ behave differently from the unit group of $M_2(\mathbb{Z}_2)$ and the unit group of $M_2(\mathbb{Z}_3)$ respectively.

2. Preliminaries and notation

Throughout, a ring will mean an associative ring with unity and for any positive integer n, $\mathbb{Z}_n$ will denote the ring of integers modulo n. For any ring R, $E(R)$ will denote the set of all idempotents in R and $\mathcal{U}(R)$, the unit group of R. For any positive integer n, $M_n(R)$ will denote the ring of $n \times n$ matrices over a ring R and $GL(n, R)$ will denote the general linear group (the group of all $n \times n$ invertible matrices over a ring R). For a commutative ring R and for every positive integer n, $SL(n, R)$ will denote the special linear group (the group of all $n \times n$ invertible matrices over the ring R that have determinant 1).

We will use standard definitions for determinant and trace of matrices over commutative rings (cf. [11]). More precisely, for a 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over a commutative ring R, determinant of A is $ad-bc$ and trace of A is $a+d$. Recall that the determinant of product of two matrices over a commutative ring is the product of the determinant of two matrices.

As in the literature, for any two integers a and b with at least one of them non-zero, gcd(a,b) will denote the greatest common divisor of a and b and for a positive

integer n, $\phi(n)$ will denote the number of positive integers less than n and relatively prime to n.

For any two elements $g_1,\ g_2$ of a group G, (g_1, g_2) will denote the commutator ${g_1}^{-1}{g_2}^{-1}g_1g_2$ of g_1 and g_2. For any group G, $\delta(G)$ will denote the group of all commutators of elements of G, called the derived subgroup of G. For any positive integer n, $\delta^{(n)}(G)$ will denote the derived subgroup of $\delta^{(n-1)}(G)$, where $\delta^{(0)}(G) = G$ and $\delta^{(1)}(G) = \delta(G)$. $\delta^{(n)}(G)$ is called the n^{th} derived subgroup of G.

A group G is said to be *solvable* of length d if its derived series is of the form $\{1\} = G_0 < G_1 < \cdots < G_d = G$ in which each factor G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, d-1$. A *metabelian group* is a group whose commutator subgroup is abelian. In fact, they are precisely the solvable groups of derived length 2.

We now give some results that will be useful in our study. We begin with the following proposition that may also be of independent interest.

Proposition 2.1. *Let R be any ring with unity and $a = \sum_{i=0}^{n} a_i x^i$ is an element in $R[x]$ such that $a^2 - a \in R$. If any of the following conditions hold:*

(1) *R has no non-zero nilpotent elements,*

(2) *$a_0 a_i = a_i a_0$ for $1 \leq i \leq n$ and $2a_0 - 1$ is a unit in R,*

then $a \in R$.

Proof. If R has no non-zero nilpotent elements and $a^2 - a \in R$, then it is easy to see that $a_i = 0$ for $1 \leq i \leq n$. The proof, in the second case, is similar to the proof of Lemma 1 in [7]. We give a brief outline for the sake of completeness. If $a \notin R$ and a_i $(i > 0)$ is the first non-zero coefficient in a, then $a^2 - a \in R$ gives $2a_0a_i - a_i = 0$. But then $a_i = 0$ as $2a_0 - 1$ is a unit in R, a contradiction. Thus $a \in R$. □

In particular, we have the following corollary.

Corollary 2.2. [7, Lemma 1] *Let R be any ring with unity and $e = \sum_{i=0}^{n} e_i x^i \in R[x]$ be an idempotent element such that e_0 commutes with e_i for $1 \leq i \leq n$. Then $e = e_0$.*

Corollary 2.3. [7, Lemma 1] *If R is an abelian ring, then $E(R[x]) = E(R)$.*

Corollary 2.4. *If R is a ring with no non-zero nilpotent elements, then $E(R[x]) = E(R)$.*

We remark that the requirement of $2a_0 - 1$ being a unit in R in Condition (2) of Proposition 2.1 cannot be dropped even when R is commutative. For example, the polynomial $a(x) = 2 + 3x$ in $\mathbb{Z}_9[x]$ satisfies the condition $a^2 - a \in \mathbb{Z}_9$ but is not in $\mathbb{Z}_9$.

Theorem 2.5. *Let R be a commutative ring. Then the trace of every non-trivial idempotent in $M_2(R)$ with determinant 0 is an idempotent.*

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a non-trivial idempotent in $M_2(R)$ and let the determinant of A is 0, that is, $ad-bc = 0$. Since A is an idempotent, $\begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Thus $a^2+bc = a$ and $bc+d^2 = d$ and hence $a^2+2bc+d^2 = a+d$. Since $ad = bc$, we have $(a+d)^2 = a+d$, that is, the trace of A is an idempotent. □

We remark that the trace of an idempotent in $M_2(R)$ with non-zero determinant need not be an idempotent. For example, the matrices $\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ in $M_2(\mathbb{Z}_6)$ are both idempotents with non-zero determinant and the trace of $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ is an idempotent whereas that of $\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ is not an idempotent.

Proposition 2.6. *Let R be a commutative ring. Then an element of $M_2(R)$ with trace 1 is an idempotent if and only if its determinant is 0.*

Proof. The result follows once we observe that the determinant of $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ is $a - a^2 - bc$ and $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$ is an idempotent if and only if $a^2 + bc = a$. □

Theorem 2.7. *Let R be a commutative ring with no non-trivial idempotents. Then the trace of every non-trivial idempotent in $M_2(R)$ is 1.*

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a non-trivial idempotent in $M_2(R)$. Then the determinant of A is also an idempotent. Since R has no non-trivial idempotents, the determinant of A is either 0 or 1. If the determinant of A is 1 then A is a unit as well as an idempotent. Thus $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a contradiction as A is a non-trivial

idempotent. If the determinant of A is 0 then, by Theorem 2.5, trace of A is an idempotent. Since R has no non-trivial idempotents, the trace of A is either 0 or 1. If the trace of A is 0 then $d = -a$. Since $ad - bc = 0$, we have $a^2 + bc = 0$ and $bc + d^2 = 0$. Hence $A^2 = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Thus A is the zero matrix, a contradiction as A is a non-trivial idempotent. Hence the trace of A is 1. □

Note that, if R is a commutative ring with non-trivial idempotents then $M_2(R)$ may have idempotents having non-idempotent trace. For example, the matrices $\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$ in $M_2(\mathbb{Z}_6)$ are both idempotents with non-idempotent trace.

Also note that the result in Theorem 2.7 does not hold for $M_3(R)$ where R is a commutative ring with unity having no non-trivial idempotents, for example, the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ in $M_3(\mathbb{Z}_3)$ is a non-trivial idempotent with trace different from 1.

Recall that, if $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_r^{m_r}}$ and for each prime p and each positive integer m, $\mathbb{Z}_{p^m}$ has no non-trivial idempotents. Thus the idempotents in $\mathbb{Z}_n$ are $(e_1, e_2, \dots, e_r)$, where $e_i = 0$ or 1 for each i. The following proposition gives precise formulas for the non-trivial idempotents in the case of 2 primes. Similar argument can be used to obtain the precise formulas for all non-trivial idempotents in the general case.

Proposition 2.8. *If p and q are distinct primes and m and n are positive integers then idempotents in $\mathbb{Z}_{p^m q^n}$ are 0, 1, $p^{kq^{n-1}(q-1)}$, and $q^{lp^{m-1}(p-1)}$ modulo $p^m q^n$, where k and l are the smallest positive integers such that $kq^{n-1}(q-1) - m$ and $lp^{m-1}(p-1) - n$ are positive.*

Proof. Let x be an idempotent in $\mathbb{Z}_{p^m q^n}$. Then $x^2 \equiv x (mod\ p^m q^n)$. Thus $x^2 \equiv x (mod\ p^m)$ and $x^2 \equiv x (mod\ q^n)$. Now $x^2 \equiv x (mod\ p^m)$ gives $x \equiv 0 (mod\ p^m)$ or $x \equiv 1 (mod\ p^m)$ and $x^2 \equiv x (mod\ q^n)$ gives $x \equiv 0 (mod\ q^n)$ or $x \equiv 1 (mod\ q^n)$.

If $x \equiv 0 (mod\ p^m)$ and $x \equiv 0 (mod\ q^n)$ then, as $\gcd(p^m, q^n) = 1$, we have $x \equiv 0 (mod\ p^m q^n)$ and if $x \equiv 1 (mod\ p^m)$ and $x \equiv 1 (mod\ q^n)$ then, as $\gcd(p^m, q^n) = 1$, we have $x \equiv 1 (mod\ p^m q^n)$. Now let $x \equiv 0 (mod\ p^m)$ and $x \equiv 1 (mod\ q^n)$ then, using

Chinese Remainder Theorem (cf. [4]) and the fact that $p^{\phi(q^n)} \equiv 1(mod\ q^n)$ (Euler's Theorem, cf. [4]), we get $x \equiv p^{kq^{n-1}(q-1)}(mod\ p^m q^n)$, where k is the smallest positive integer such that $kq^{n-1}(q-1)-m$ is positive . Similarly if $x \equiv 1(mod\ p^m)$ and $x \equiv 0(mod\ q^n)$ then $x \equiv q^{lp^{m-1}(p-1)}(mod\ p^m q^n)$, where l is the smallest positive integer such that $lp^{m-1}(p-1)-n$ is positive. Thus the only idempotents in $\mathbb{Z}_{p^m q^n}$ are $0, 1, p^{kq^{n-1}(q-1)}$ and $q^{lp^{m-1}(p-1)}$ modulo $p^m q^n$ where k and l are the smallest positive integers such that $kq^{n-1}(q-1)-m$ and $lp^{m-1}(p-1)-n$ are positive. □

As a particular case of Proposition 2.8, it follows that if p and q are distinct primes then the idempotents in $\mathbb{Z}_{pq}$ are $0,\ 1,\ p^{q-1},\ q^{p-1}$ modulo pq and if p and q are distinct primes such that $q > p$ then the idempotents in $\mathbb{Z}_{p^2q}$ are $0,\ 1,\ p^{q-1},\ q^{p(p-1)}$ modulo p^2q and those in $\mathbb{Z}_{p^3q}$ are $0,\ 1,\ p^{2(q-1)},\ q^{p^2(p-1)}$ modulo p^3q.

3. Idempotents in matrix rings over polynomial rings

In this section, we give conditions such that a matrix in $M_2(R[x])$, where R is a commutative ring, is an idempotent and use it to give the form of idempotents in $M_2(\mathbb{Z}_p[x])$, where p is a prime, $M_2(\mathbb{Z}_{2p}[x])$, where p is an odd prime, and $M_2(\mathbb{Z}_{3p}[x])$, where p is a prime greater than 3. We first prove the following proposition.

Proposition 3.1. *If R is a reduced commutative ring then the determinant as well as the trace of every idempotent in $M_2(R[x])$ is in R.*

Proof. Suppose R is a reduced commutative ring and let $A = \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ be an idempotent in $M_2(R[x])$. For convenience, we will write $a,\ b,\ c,\ d$ for $a(x),\ b(x),\ c(x),\ d(x)$ respectively. Since A is an idempotent, determinant of A is an idempotent in $R[x]$. Since R is commutative, idempotents in $R[x]$ are precisely the idempotents in R. Hence determinant of A is an idempotent in R, that is, $ad - bc \in R$. Again, as A is an idempotent, we have $a^2 + bc = a$, $b(a + d) = b$, $c(a+d) = c$, and $bc+d^2 = d$. Thus $(a+d)^2 = a+d+2(ad-bc)$. Since $ad-bc \in R$, we have $(a+d)^2 - (a+d) \in R$. Hence, by Proposition 2.1, $a+d \in R$, that is, trace of A is in R. □

Since for a commutative ring R, the idempotents in the polynomial ring $R[x]$ over R are precisely the idempotents in R and for a commutative ring R with no non-trivial idempotents, trace of every non-trivial idempotent in $M_2(R)$ is 1 (Theorem 2.7), we have the following proposition.

Proposition 3.2. *Let R be a commutative ring with no non-trivial idempotents. Then the non-trivial idempotents of $M_2(R[x])$ are of the form* $\begin{pmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{pmatrix}$, *where $a(x),\ b(x),\ c(x) \in R[x]$, not necessarily non-zero, such that $a(x)(1-a(x)) = b(x)c(x)$.*

Since for any prime p, $\mathbb{Z}_p[x]$ has no non-trivial idempotents, we have the following corollary.

Corollary 3.3. *For any prime p, the non-trivial idempotents of $M_2(\mathbb{Z}_p[x])$ are of the form* $\begin{pmatrix} t(x) & q(x) \\ r(x) & 1-t(x) \end{pmatrix}$, *where $q(x),\ r(x),\ t(x) \in \mathbb{Z}_p[x]$, not necessarily non-zero, such that $t(x)\{1-t(x)\} = q(x)r(x)$.*

We now obtain conditions under which a matrix in $M_2(\mathbb{Z}_{2p}[x])$, where p is an odd prime, is an idempotent and use this to give the form of idempotents in $M_2(\mathbb{Z}_{2p}[x])$. We first prove the following proposition.

Proposition 3.4. *For any odd prime p and any non-trivial idempotent A in $M_2(\mathbb{Z}_{2p}[x])$, one of the following holds:*

(1) *determinant of A is 0 and trace of A is either 1 or p or $p+1$,*
(2) *determinant of A is p and trace of A is either 0 or $p+1$,*
(3) *determinant of A is $p+1$ and trace of A is either 2 or $p+2$.*

In particular, the same holds for the idempotents in $M_2(\mathbb{Z}_{2p})$.

Proof. First note that the idempotents in $\mathbb{Z}_{2p}$ are 0, 1, p, and 2^{p-1} (Proposition 2.8). Since for any odd prime p, $2^{p-1} \equiv (p+1)(mod\ 2p)$ and the idempotents in $\mathbb{Z}_{2p}[x]$ are precisely the idempotents in $\mathbb{Z}_{2p}$, the idempotents in $\mathbb{Z}_{2p}[x]$ are 0, 1, p, and $p+1$. Now let $A = \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ be a non-trivial idempotent of $M_2(\mathbb{Z}_{2p}[x])$. For convenience, we will write $a,\ b,\ c,\ d$ for $a(x),\ b(x),\ c(x),\ d(x)$ respectively. Since A is an idempotent, we have $a^2 + bc = a$, $b(a+d) = b$, $c(a+d) = c$, and $bc + d^2 = d$ and determinant of A is an idempotent in $\mathbb{Z}_{2p}$ (Proposition 3.1). Thus, determinant of A is 0 or 1 or p or $p+1$. If determinant of A is 1 then $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a trivial idempotent in $M_2(\mathbb{Z}_{2p}[x])$. Hence, the determinant of A is 0 or p or $p+1$. Also, trace of A is in $\mathbb{Z}_{2p}$ (Proposition 3.1), that is, $a + d \in \mathbb{Z}_{2p}$.

Case 1: Determinant of A is 0. In this case, by Theorem 2.5 and Proposition 3.1, trace of A is an idempotent in $\mathbb{Z}_{2p}$. Thus $a+d$ is either 0 or 1 or p or $p+1$. If $a+d = 0$

then, as in Theorem 2.7, A is the zero matrix in $M_2(\mathbb{Z}_{2p}[x])$, a contradiction as A is a non-trivial idempotent.

Note that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} p+1 & 0 \\ 0 & 0 \end{pmatrix}$ in $M_2(\mathbb{Z}_{2p}[x])$ have determinant 0 and trace 1, p, $p+1$ respectively.

Case 2: Determinant of A is p. In this case, $ad-bc=p$, $a^2+bc=a$, and $bc+d^2=d$ give $(a+d)^2=a+d$, that is, $a+d$ is an idempotent. Since $a+d\in\mathbb{Z}_{2p}$, $a+d$ is either 0 or 1 or p or $p+1$. We claim that $a+d$ is 0 or $p+1$.

If $a+d=1$ then $ad-bc=p$ gives $a^2+bc=-p+a(mod\ 2p)$ and hence $A^2=\begin{pmatrix} -p+a & b \\ c & 1+p-a \end{pmatrix}$. Since A is an idempotent, we get $-p+a=a$, a contradiction.

If $a+d=p$ then $ad-bc=p$ gives $a^2+bc=pa-p$ and hence $A^2=\begin{pmatrix} pa-p & pb \\ pc & p^2+p-pa \end{pmatrix}$. Since A is an idempotent, we get $(p-1)a=p$. Thus $(p-1)a_0=p(mod\ 2p)$ where a_0 is the term without x in a. This is not possible as $\gcd(p-1,2p)=2$ and 2 does not divide p.

Note that the matrices $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ in $\mathbb{M}_2(\mathbb{Z}_{2p}[x])$ have determinant p and trace 0, $p+1$ respectively.

Case 3: Determinant of A is $p+1$. In this case, $ad-bc=p+1$, $a^2+bc=a$, and $bc+d^2=d$ give $(a+d)^2=a+d+2$. Since $a+d\in\mathbb{Z}_{2p}$, we get $a+d$ is either 2 or -1 or $p-1$ or $p+2$.

We claim that the cases $a+d=-1$ and $a+d=p-1$ are not possible if $p\neq 3$. Note that the cases $a+d=-1$ and $a+d=p-1$ coincides with the cases $a+d=p+2$ and $a+d=2$ respectively when $p=3$. Let $p\neq 3$.

If $a+d=p-1$, then $d=p-1-a$ and hence $ad-bc=p+1$ gives $a^2+bc=pa-a-p-1$. Thus $A^2=\begin{pmatrix} pa-1-a-p & (p-1)b \\ (p-1)c & (p+1)a \end{pmatrix}$. Since A is an idempotent, we have $(p-2)b=0$ and $(p-2)c=0$. Since $\gcd(p-2,2p)=1$, we get $b=c=0$ and hence $A=\begin{pmatrix} a & 0 \\ 0 & p-1-a \end{pmatrix}$. Since A is an idempotent, both a and $p-1-a$ must be idempotents in $\mathbb{Z}_{2p}[x]$ and hence in $\mathbb{Z}_{2p}$. Thus, using $a^2=a$ and $(p-1-a)^2=p-1-a$, we get $4a\equiv -2(mod\ 2p)$. Since a, being an idempotent in $\mathbb{Z}_{2p}$, is either 0 or 1 or p or $p+1$, it is easy to see that none of the values of a satisfy $4a\equiv -2(mod\ 2p)$.

If $a+d=-1$, then $A^2=\begin{pmatrix} a^2+bc & -b \\ -c & bc+d^2 \end{pmatrix}$. Since A is an idempotent, we get $a^2+bc=a$, $2b=0$, and $2c=0$. Hence $4a^2=4a$. Also, as $ad-bc=p+1$, we have $a(-1-a)-bc=p+1$ and hence $2a=p+1$ as $a^2+bc=a$. Now $4a^2-4a=0$ gives $(p-1)^2-2(p-1)=0$. Thus, $p+3\equiv 0(mod\ 2p)$, which is not possible as p does not divide 3.

Note that the matrices $\begin{pmatrix} p+1 & 0 \\ 0 & p+1 \end{pmatrix}$ and $\begin{pmatrix} p+1 & 0 \\ 0 & 1 \end{pmatrix}$ in $M_2(\mathbb{Z}_{2p}[x])$ have determinant $p+1$ and trace 2 and $p+2$, respectively. □

Theorem 3.5. *For any odd prime p, any non-trivial idempotent in $M_2(\mathbb{Z}_{2p}[x])$ is of one of the following forms:*

(1) $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \begin{pmatrix} p+1 & 0 \\ 0 & p+1 \end{pmatrix}$

(2) $\begin{pmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{pmatrix}$, *where* $a(x)\{1-a(x)\}-b(x)c(x)=0$

(3) $\begin{pmatrix} pa(x) & pb(x) \\ pc(x) & p(1-a(x)) \end{pmatrix}$, *where* $a(x)\{1-a(x)\}-b(x)c(x)=2f(x)$

(4) $\begin{pmatrix} 2a(x) & 2b(x) \\ 2c(x) & p+1-2a(x) \end{pmatrix}$, *where* $a(x)\{1-2a(x)\}-2b(x)c(x)=pg(x)$

(5) $\begin{pmatrix} p+2a(x) & 2b(x) \\ 2c(x) & 1-2a(x) \end{pmatrix}$, *where* $a(x)\{1-2a(x)\}-2b(x)c(x)=ph(x)$

(6) $\begin{pmatrix} 1+pa(x) & pb(x) \\ pc(x) & p+1-pa(x) \end{pmatrix}$, *where* $a(x)\{1-a(x)\}-b(x)c(x)=2\phi(x)$,

where $a(x)$, $b(x)$, $c(x)$, $f(x)$, $g(x)$, $h(x)$, and $\phi(x)$ are polynomials in $\mathbb{Z}_{2p}[x]$, not necessarily non-zero.

Proof. It is easy to check that the matrices in (1)–(6) with the given conditions are idempotents in $M_2(\mathbb{Z}_{2p}[x])$, so we are only left to prove that every idempotent in $M_2(\mathbb{Z}_{2p}[x])$ has one of the stated forms. Let $A=\begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ be an idempotent in $M_2(\mathbb{Z}_{2p}[x])$. Then, by Proposition 3.4, one of the following holds:

(1) determinant of A is 0 and trace of A is either 1 or p or $p+1$,
(2) determinant of A is p and trace of A is either 0 or $p+1$,
(3) determinant of A is $p+1$ and trace of A is either 2 or $p+2$.

We first consider the case when determinant of A is 0. In this case, trace of A is either 1 or p or $p+1$, that is, $a+d$ is either 1 or p or $p+1$.

If $a+d=1$, then $d=1-a$ and hence $ad-bc=0$ gives $a^2+bc=a$. Also $(a+d)b=b$, $(a+d)c=c$, and $bc+d^2=1-a$. Thus, $A^2=\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$. Thus, in this case, $A=\begin{pmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-a(x)\}=b(x)c(x)$.

If $a+d=p$, then $d=p-a$ and hence $ad-bc=0$ gives $a^2+bc=pa$. Thus $A^2=\begin{pmatrix} pa & pb \\ pc & p-pa \end{pmatrix}$. Since A is an idempotent, $(p-1)a=0$, $(p-1)b=0$, and $(p-1)c=0$. Therefore, $a=pa'(x)$, $b=pb'(x)$, and $c=pc'(x)$, where $a'(x)$, $b'(x)$ and $c'(x)$ are polynomials in $\mathbb{Z}_{2p}[x]$. Now since $ad-bc=0$, we get $pa'(x)\{1-a'(x)\}=pb'(x)c'(x)$, which is equivalent to $a'(x)\{1-a'(x)\}-b'(x)c'(x)=2f(x)$ for some polynomial $f(x)\in\mathbb{Z}_{2p}[x]$. Hence, $A=\begin{pmatrix} pa(x) & pb(x) \\ pc(x) & p(1-a(x)) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-a(x)\}-b(x)c(x)=2f(x)$ for some $f(x)\in\mathbb{Z}_{2p}[x]$.

If $a+d=p+1$, then $d=p+1-a$ and hence $ad-bc=0$ gives $a^2+bc=(p+1)a$. Thus, $A^2=\begin{pmatrix} (p+1)a & (p+1)b \\ (p+1)c & pa+p-a+1 \end{pmatrix}$. Since A is an idempotent, $pa=0$, $pb=0$, and $pc=0$. Hence, as in the previous case, $A=\begin{pmatrix} 2a(x) & 2b(x) \\ 2c(x) & p+1-2a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-2a(x)\}-2b(x)c(x)=pg(x)$ for some $g(x)\in\mathbb{Z}_{2p}[x]$.

Next, we consider the case where determinant of A is p. In this case trace of A is either 0 or $p+1$, that is, $a+d$ is either 0 or $p+1$.

It is easy to see that the determinant of $(A+pI)$ is 0 and the trace of $(A+pI)$ is trace of A. Therefore, by the previous case, $A+pI$ is either the zero matrix in $M_2(\mathbb{Z}_{2p}[x])$ or $\begin{pmatrix} 2a(x) & 2b(x) \\ 2c(x) & p+1-2a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-2a(x)\}-2b(x)c(x)=pg(x)$. Hence A is $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$ or $\begin{pmatrix} p+2a(x) & 2b(x) \\ 2c(x) & 1-2a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-2a(x)\}-2b(x)c(x)=ph(x)$ for some $h(x)\in\mathbb{Z}_{2p}[x]$.

Finally, we consider the case where determinant of A is $p+1$. In this case, trace of A is either 2 or $p+2$, that is, $a+d$ is either 2 or $p+2$.

If $a+d=2$, then $d=2-a$ and hence $ad-bc=p+1$ gives $a^2+bc=2a-p-1$. Thus $A^2=\begin{pmatrix} 2a-p-1 & 2b \\ 2c & 3+p-2a \end{pmatrix}$. Since A is an idempotent, we get $a=p+1$, $b=c=0$. Thus $A=\begin{pmatrix} p+1 & 0 \\ 0 & p+1 \end{pmatrix}$.

If $a+d=p+2$, then $d=p+2-a$ and hence $ad-bc=p+1$ gives $a^2+bc=2a+pa-p-1$. Thus $A^2=\begin{pmatrix} 2a+pa-p-1 & (p+2)b \\ (p+2)c & 3+pa-2a \end{pmatrix}$. Since A is an idempotent, we have $(p+1)a=p+1$, $(p+1)b=0$, and $(p+1)c=0$. Hence, as earlier, $A=\begin{pmatrix} 1+pa(x) & pb(x) \\ pc(x) & p+1-pa(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{2p}[x]$ such that $a(x)\{1-a(x)\}-b(x)c(x)=2\phi(x)$ for some $\phi(x)\in\mathbb{Z}_{2p}[x]$. □

Note that all computations in Proposition 3.4 and Theorem 3.5 are modulo $2p$, even if it is not explicitly stated. We also observe that every idempotent of form 3 in Theorem 3.5 is orthogonal to every idempotent of form 4.

Proposition 3.6. *For any prime p greater than 3 and any non-trivial idempotent A in $M_2(\mathbb{Z}_{3p}[x])$, one of the following holds:*

(1) *determinant of A is 0 and trace of A is either 1 or p^2 or 3^{p-1},*
(2) *determinant of A is 3^{p-1} and trace of A is either $3^{p-1}+1$ or $2\cdot 3^{p-1}$,*
(3) *determinant of A is p^2 and trace of A is either $2p^2$ or p^2+1.*

In particular, the same holds for the idempotents in $M_2(\mathbb{Z}_{3p})$.

Proof. First note that the idempotents in $\mathbb{Z}_{3p}$ are 0, 1, p^2, and 3^{p-1} modulo $3p$ (Proposition 2.8). Thus the idempotents in $\mathbb{Z}_{3p}[x]$, being same as the idempotents in $\mathbb{Z}_{3p}$, are 0, 1, p^2, and 3^{p-1} modulo $3p$. Now let $A=\begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ be a non-trivial idempotent of $M_2(\mathbb{Z}_{3p}[x])$. For convenience, we will write $a,\ b,\ c,\ d$ for $a(x),\ b(x),\ c(x),\ d(x)$ respectively. Since A is an idempotent, we have $a^2+bc=a$, $b(a+d)=b$, $c(a+d)=c$, and $bc+d^2=d$. Also, as determinant of A is an idempotent in $\mathbb{Z}_{3p}$ (Proposition 3.1), determinant of A is 0 or 1 or p^2 or 3^{p-1} modulo $3p$. If determinant of A is 1, then $A=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, a trivial idempotent in $M_2(\mathbb{Z}_{3p}[x])$. Hence determinant of A is 0 or p^2 or 3^{p-1} modulo $3p$. Also, by Proposition 3.1, trace of A is in $\mathbb{Z}_{3p}$, that is, $a+d\in\mathbb{Z}_{3p}$.

Case 1: Determinant of A is 0. In this case, by Theorem 2.5, trace of A is an idempotent in $\mathbb{Z}_{3p}[x]$ and hence in $\mathbb{Z}_{3p}$. Thus $a+d$ is either 0 or 1 or p^2 or

3^{p-1}. If $a+d=0$ then, as in Theorem 2.7, A is the zero matrix in $M_2(\mathbb{Z}_{3p}[x])$, a contradiction as A is a non-trivial idempotent.

Note that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} p^2 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 3^{p-1} & 0 \\ 0 & 0 \end{pmatrix}$ in $M_2(\mathbb{Z}_{3p}[x])$ have determinant 0 and trace 1, p^2, 3^{p-1} respectively.

Case 2: Determinant of A is 3^{p-1}. In this case, $ad-bc=3^{p-1}$, $a^2+bc=a$, and $bc+d^2=d$ give $(a+d)^2=a+d+2\cdot 3^{p-1}(mod\ 3p)$. Since $a+d\in\mathbb{Z}_{3p}$, we get $a+d$ is either $3^{p-1}+1$ or $2\cdot 3^{p-1}$ or -3^{p-1} or $1-2\cdot 3^{p-1}$. We claim that the cases $a+d=-3^{p-1}$ and $a+d=1-2\cdot 3^{p-1}$ are not possible.

If $a+d=-3^{p-1}$, then $d=-3^{p-1}-a$ and hence $ad-bc=3^{p-1}$ gives $a^2+bc=-3^{p-1}a-3^{p-1}$. Thus $A^2=\begin{pmatrix} -3^{p-1}a-3^{p-1} & -3^{p-1}b \\ -3^{p-1}c & 3^{p-1}a \end{pmatrix}$. Since A is an idempotent, we have $(3^{p-1}+1)b=0$ and $(3^{p-1}+1)c=0$. Since $\gcd(3^{p-1}+1,3p)=1$ we get $b=c=0$. Thus $A=\begin{pmatrix} a & 0 \\ 0 & -3^{p-1}-a \end{pmatrix}$. Since A is an idempotent, both a and $-3^{p-1}-a$ must be idempotents in $\mathbb{Z}_{3p}[x]$ and hence in $\mathbb{Z}_{3p}$. Hence this case is not possible, as $-3^{p-1}-a$ is not an idempotent for $a=0,\ 1,\ p^2,$ and 3^{p-1}.

If $a+d=1-2\cdot 3^{p-1}$, then $A^2=\begin{pmatrix} a^2+bc & (1-2\cdot 3^{p-1})b \\ (1-2\cdot 3^{p-1})c & bc+d^2 \end{pmatrix}$. Since A is an idempotent, we get $a^2+bc=a$, $2\cdot 3^{p-1}b=0$, and $2\cdot 3^{p-1}c=0$. Thus $(2\cdot 3^{p-1}a)^2-2(2\cdot 3^{p-1}a)=0$. Also, as $ad-bc=3^{p-1}$, we have $a(1-2\cdot 3^{p-1}-a)-bc=3^{p-1}$ and hence $2\cdot 3^{p-1}a=-3^{p-1}$ as $a^2+bc=a$. Now $(2\cdot 3^{p-1}a)^2-2(2\cdot 3^{p-1}a)=0$ gives $(-3^{p-1})^2-2(-3^{p-1})=0$. Thus $3^p\equiv 0\ (mod\ 3p)$, which is not possible as $3^p\equiv 3\ (mod\ 3p)$.

Note that the matrices $\begin{pmatrix} 3^{p-1} & 0 \\ 0 & 3^{p-1} \end{pmatrix}$ and $\begin{pmatrix} 3^{p-1} & 0 \\ 0 & 1 \end{pmatrix}$ in $M_2(\mathbb{Z}_{3p}[x])$ have determinant 3^{p-1} and trace $2\cdot 3^{p-1}$ and $3^{p-1}+1$, respectively.

Case 3: Determinant of A is p^2. In this case, $ad-bc=p^2$, $a^2+bc=a$, and $bc+d^2=d$ give $(a+d)^2=a+d+2p^2(mod\ 3p)$.

If $p\equiv 1(mod\ 3)$, then $p^2\equiv p(mod\ 3p)$. Therefore, $(a+d)^2=a+d+2p(mod\ 3p)$. Since $a+d\in\mathbb{Z}_{3p}$, $a+d$ is either $2p$ or $p+1$.

Note that the matrices $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$, $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ in $M_2(\mathbb{Z}_{3p}[x])$ have determinant $p^2\equiv p(mod\ 3p)$ and trace $2p\equiv p^2(mod\ 3p)$, $p+1\equiv p^2+1(mod\ 3p)$, respectively.

If $p\equiv 2(mod\ 3)$, then $p^2\equiv 2p(mod\ 3p)$ and hence $2p^2\equiv p(mod\ 3p)$. Therefore, $(a+d)^2=a+d+p(mod\ 3p)$. Since $a+d\in\mathbb{Z}_{3p}$, $a+d$ is either p or $2p+1$.

Note that the matrices $\begin{pmatrix} 2p & 0 \\ 0 & 2p \end{pmatrix}, \begin{pmatrix} 2p & 0 \\ 0 & 1 \end{pmatrix}$ have determinant $p^2 \equiv 2p(mod\ 3p)$ and trace $p \equiv 2p^2(mod\ 3p)$, $2p+1 \equiv p^2+1(mod\ 3p)$, respectively. □

Theorem 3.7. *For any odd prime p greater than 3, any non-trivial idempotent in* $M_2(\mathbb{Z}_{3p}[x])$ *is of one of the following forms:*

(1) $\begin{pmatrix} 3^{p-1} & 0 \\ 0 & 3^{p-1} \end{pmatrix}, \begin{pmatrix} p^2 & 0 \\ 0 & p^2 \end{pmatrix}$

(2) $\begin{pmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{pmatrix}$, *where* $a(x)\{1-a(x)\} - b(x)c(x) = 0$

(3) $\begin{pmatrix} p^2a(x) & p^2b(x) \\ p^2c(x) & p^2(1-a(x)) \end{pmatrix}$, *where* $a(x)\{1-a(x)\} - b(x)c(x) = 3f(x)$

(4) $\begin{pmatrix} 3^{p-1}a(x) & 3^{p-1}b(x) \\ 3^{p-1}c(x) & 3^{p-1}(1-a(x)) \end{pmatrix}$, *where* $a(x)\{1-a(x)\} - b(x)c(x) = pg(x)$

(5) $\begin{pmatrix} 1+pa(x) & pb(x) \\ pc(x) & 3^{p-1}-pa(x) \end{pmatrix}$, *where* $a(x)\{1+pa(x)\} + pb(x)c(x) = 3h(x)$

(6) $\begin{pmatrix} p^2+3a(x) & 3b(x) \\ 3c(x) & 1-3a(x) \end{pmatrix}$, *where* $a(x)\{1-3a(x)\} - 3b(x)c(x) = p\phi(x)$,

where $a(x)$, $b(x)$, $c(x)$, $f(x)$, $g(x)$, $h(x)$, *and* $\phi(x)$ *are polynomials in* $\mathbb{Z}_{3p}[x]$, *not necessarily non-zero.*

Proof. It is easy to check that the matrices in (1)-(6) with the given conditions are idempotents in $M_2(\mathbb{Z}_{3p}[x])$, so we are now left to prove that every idempotent in $M_2(\mathbb{Z}_{3p}[x])$ has one of the stated forms. Let $A = \begin{pmatrix} a(x) & b(x) \\ c(x) & d(x) \end{pmatrix}$ be an idempotent in $M_2(\mathbb{Z}_{3p}[x])$.

Then, by Proposition 3.6, one of the following holds:

(1) determinant of A is 0 and trace of A is either 1 or p^2 or 3^{p-1},
(2) determinant of A is 3^{p-1} and trace of A is either $3^{p-1}+1$ or $2\cdot 3^{p-1}$,
(3) determinant of A is p^2 and trace of A is either $2p^2$ or p^2+1.

We first consider the case when determinant of A is 0. In this case, trace of A is either 1 or p^2 or 3^{p-1}, that is, $a+d$ is either 1 or p^2 or 3^{p-1}.

If $a+d=1$, then $d=1-a$ and hence $ad-bc=0$ gives $a^2+bc=a$. Also, $(a+d)b=b$, $(a+d)c=c$, and $bc+d^2=1-a$. Thus, $A^2 = \begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$. Hence, in this case, $A = \begin{pmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x) \in \mathbb{Z}_{3p}[x]$ such that $a(x)\{1-a(x)\} = b(x)c(x)$.

If $a+d=p^2$, then $d=p^2-a$ and hence $ad-bc=0$ gives $a^2+bc=p^2a$. Thus, $A^2=\begin{pmatrix} p^2a & p^2b \\ p^2c & p^2(1-a) \end{pmatrix}$. Since A is an idempotent, we get $(p^2-1)a=0$, $(p^2-1)b=0$, and $(p^2-1)c=0$, that is, $a,\ b,\ c$ belong to the annihilator of p^2-1 in $\mathbb{Z}_{3p}[x]$. Therefore, as p^2 is an idempotent in $\mathbb{Z}_{3p}$, $a=p^2a'(x)$, $b=p^2b'(x)$, and $c=p^2c'(x)$, where $a'(x)$, $b'(x)$, and $c'(x)$ are polynomials in $\mathbb{Z}_{3p}[x]$. Now, since $ad-bc=0$, we get $p^2a'(x)\{1-a'(x)\}=p^2b'(x)c'(x)$, which is equivalent to $a'(x)\{1-a'(x)\}-b'(x)c'(x)=3f(x)$ for some $f(x)\in\mathbb{Z}_{3p}[x]$. Hence $A=\begin{pmatrix} p^2a(x) & p^2b(x) \\ p^2c(x) & p^2(1-a(x)) \end{pmatrix}$, where $a(x), b(x), c(x)\in\mathbb{Z}_{3p}[x]$ such that $a(x)\{1-a(x)\}-b(x)c(x)=3f(x)$ for some $f(x)\in\mathbb{Z}_{3p}[x]$.

If $a+d=3^{p-1}$, then $d=3^{p-1}-a$ and hence $ad-bc=0$ gives $a^2+bc=3^{p-1}a$. Thus $A^2=\begin{pmatrix} 3^{p-1}a & 3^{p-1}b \\ 3^{p-1}c & 3^{p-1}(1-a) \end{pmatrix}$. Since A is an idempotent, we get $(3^{p-1}-1)a=0$, $(3^{p-1}-1)b=0$ and $(3^{p-1}-1)c=0$. Hence, as in the previous case, $A=\begin{pmatrix} 3^{p-1}a(x) & 3^{p-1}b(x) \\ 3^{p-1}c(x) & 3^{p-1}(1-a(x)) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{3p}[x]$ such that $a(x)\{1-a(x)\}-b(x)c(x)=pg(x)$ for some $g(x)\in\mathbb{Z}_{3p}[x]$.

Next, we consider the case, where determinant of A is 3^{p-1}. In this case, trace of A is $2\cdot3^{p-1}$ or $1+3^{p-1}$ modulo $3p$, that is, $a+d$ is $2\cdot3^{p-1}$ or $1+3^{p-1}$ modulo $3p$.

If $a+d=2\cdot3^{p-1}$, then $d=2\cdot3^{p-1}-a$ and hence $ad-bc=3^{p-1}$ gives $a^2+bc=2\cdot3^{p-1}a-3^{p-1}$. Thus $A^2=\begin{pmatrix} 2\cdot3^{p-1}a-3^{p-1} & 2\cdot3^{p-1}b \\ 2\cdot3^{p-1}c & 3^p-2\cdot3^{p-1}a \end{pmatrix}$. Since A is an idempotent, we get $(2\cdot3^{p-1}-1)b=0$ and $(2\cdot3^{p-1}-1)c=0$. Since 3^{p-1} is an idempotent, $2\cdot3^{p-1}-1$ is a unit. Thus $b=c=0$. Therefore, $A=\begin{pmatrix} a & 0 \\ 0 & 2\cdot3^{p-1}-a \end{pmatrix}$. Since A is an idempotent, both a and $2\cdot3^{p-1}-a$ must be idempotents in $\mathbb{Z}_{3p}[x]$ and hence in $\mathbb{Z}_{3p}$. Thus $a=3^{p-1}$ as $2\cdot3^{p-1}-a$ is not an idempotent for $a=0,\ 1$ and p^2. Hence $A=\begin{pmatrix} 3^{p-1} & 0 \\ 0 & 3^{p-1} \end{pmatrix}$.

If $a+d=1+3^{p-1}$, then $d=3^{p-1}+1-a$ and hence $ad-bc=3^{p-1}$ gives $a^2+bc=3^{p-1}a+a-3^{p-1}$. Thus, $A^2=\begin{pmatrix} 3^{p-1}a+a-3^{p-1} & (3^{p-1}+1)b \\ (3^{p-1}+1)c & 1+2\cdot3^{p-1}-(3^{p-1}+1)a \end{pmatrix}$. Since A is an idempotent, we get $3^{p-1}a=3^{p-1}$, $3^{p-1}b=0$, and $3^{p-1}c=0$. Thus, $A=\begin{pmatrix} 1+pa(x) & pb(x) \\ pc(x) & 3^{p-1}-pa(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x)\in\mathbb{Z}_{3p}[x]$ such that $a(x)\{1+a(x)\}+pb(x)c(x)=3h(x)$ for some $h(x)\in\mathbb{Z}_{3p}[x]$.

Finally, we consider the case where determinant of A is p^2. In this case, trace of A is either $2p^2$ or p^2+1 modulo $3p$, that is, $a+d$ is either $2p^2$ or p^2+1 modulo $3p$.

If $p \equiv 1(mod\ 3)$ then, as $p^2 \equiv p(mod\ 3p)$, $a+d$ is either $2p$ or $p+1$.

If $a+d=2p$, then $d=2p-a$ and hence $ad-bc=p^2 \equiv p(mod\ 3p)$ gives $a^2+bc \equiv (2a-1)p(mod\ 3p)$. Thus $A^2 = \begin{pmatrix} (2a-1)p & 2pb \\ 2pc & -2pa \end{pmatrix}$. Since A is an idempotent, we get $(2p-1)b=0$ and $(2p-1)c=0$. Now, as p is an idempotent, $2p-1$ is a unit. Thus $b=c=0$. Therefore, $A = \begin{pmatrix} a & 0 \\ 0 & 2p-a \end{pmatrix}$. Since A is an idempotent, both a and $2p-a$ must be idempotents in $\mathbb{Z}_{3p}[x]$ and hence in $\mathbb{Z}_{3p}$. Thus, $a=p$, as $2p-a$ is not an idempotent for $a=0,\ 1,$ and 3^{p-1}. Hence $A = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$.

If $a+d=p+1$, then $d=p+1-a$ and hence $ad-bc=p^2 \equiv p(mod\ 3p)$ gives $a^2+bc = pa+a-p(mod\ 3p)$. Thus, $A^2 = \begin{pmatrix} pa+a-p & (p+1)b \\ (p+1)c & 1+2p-(p+1)a \end{pmatrix}$. Since A is an idempotent, we get $pa=p$, $pb=0$, and $pc=0$. Thus, $A = \begin{pmatrix} p+3a(x) & 3b(x) \\ 3c(x) & 1-3a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x) \in \mathbb{Z}_{3p}[x]$ such that $a(x)\{1-3a(x)\}-3b(x)c(x)=p\phi(x)$ for some $\phi(x) \in \mathbb{Z}_{3p}[x]$.

If $p \equiv 2(mod\ 3)$ then, as $p^2 \equiv 2p(mod\ 3p)$, $a+d$ is either p or $2p+1$.

If $a+d=p$, then $d=p-a$ and hence $ad-bc=p^2 \equiv 2p(mod\ 3p)$ gives $a^2+bc \equiv pa+p(mod\ 3p)$. Thus $A^2 = \begin{pmatrix} pa+p & pb \\ pc & 2pa \end{pmatrix}$. Since A is an idempotent, we get $(p-1)b=0$ and $(p-1)c=0$. Now, as $2p$ is an idempotent, $p-1=2(2p)-1$ is a unit. Thus $b=c=0$. Therefore, $A = \begin{pmatrix} a & 0 \\ 0 & p-a \end{pmatrix}$. Since A is an idempotent, both a and $p-a$ must be idempotents in $\mathbb{Z}_{3p}[x]$ and hence in $\mathbb{Z}_{3p}$. Thus, $a=p^2 \equiv 2p(mod\ 3p)$, as $p-a$ is not an idempotent for $a=0,\ 1,$ and 3^{p-1}. Hence $A = \begin{pmatrix} 2p & 0 \\ 0 & 2p \end{pmatrix}$.

If $a+d=2p+1$, then $d=2p+1-a$ and hence $ad-bc=p^2 \equiv 2p(mod\ 3p)$ gives $a^2+bc=2pa+a-2p(mod\ 3p)$. Thus, $A^2 = \begin{pmatrix} 2pa+a-2p & (2p+1)b \\ (2p+1)c & 1+p-(2p+1)a \end{pmatrix}$. Since A is an idempotent, we get $2pa=2p$, $2pb=0$ and $2pc=0$. Thus, $A = \begin{pmatrix} 2p+3a(x) & 3b(x) \\ 3c(x) & 1-3a(x) \end{pmatrix}$, where $a(x),\ b(x),\ c(x) \in \mathbb{Z}_{3p}[x]$ such that $a(x)\{1-3a(x)\}-3b(x)c(x)=p\zeta(x)$ for some $\zeta(x) \in \mathbb{Z}_{3p}[x]$.

Hence, in this case, any idempotent is either $\begin{pmatrix} p^2 & 0 \\ 0 & p^2 \end{pmatrix}$ or have the form $\begin{pmatrix} p^2+3a(x) & 3b(x) \\ 3c(x) & 1-3a(x) \end{pmatrix}$, where $a(x)\{1-3a(x)\}-3b(x)c(x)=p\phi(x)$. □

Note that all computations in Proposition 3.6 and Theorem 3.7 are modulo $3p$, even if it is not explicitly stated. We also observe that every idempotent of form 3 in Theorem 3.7 is orthogonal to every idempotent of form 4.

4. Units in matrix rings over polynomial rings

In this section, we consider the unit groups of $M_2(\mathbb{Z}_2[x])$ and $M_2(\mathbb{Z}_3[x])$. We first show that for any ring R, the unit group of the $n \times n$ matrix ring, $M_n(R[x])$ over $R[x]$ is not solvable. Since every non-trivial polynomial ring $R[x]$ can be mapped onto a large finite field and except for a few exceptions of finite fields $\mathbb{F}$, the group $SL(n,\mathbb{F})$ is a nonabelian simple group for $n \geq 2$, one may deduce that $GL(n, R[x])$ is not solvable. We, however, give a direct proof. For the sake of simplicity we give proof in the case $n = 2$. The argument can be extended to any value of $n \geq 2$ by replacing each element A in the set $\mathcal{L}$ in Proposition 4.1 with the block matrix $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ and each polynomial $p(x)$ in the proof of the proposition with the block matrix $\begin{pmatrix} p(x) & 0 \\ 0 & I \end{pmatrix}$ where each 0 is a zero matrix of the appropriate size and I is the identity matrix of the appropriate size. We begin with the following proposition.

Proposition 4.1. *Let R be any ring and let*

$$\mathcal{L} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Then, for each $A \in \mathcal{L}$ there exist units $p = p(x),\ q = q(x) \in M_2(R[x])$ such that either the leading coefficient of p or that of p^{-1} and the leading coefficient of q or that of q^{-1} is in the set $\mathcal{L}$; the leading coefficient of the commutator (p, q) of p and q is A and the degree of (p, q) is equal to the sum of degrees of $p,\ q,\ p^{-1},\ q^{-1}$.

Proof. Recall that if the product of leading coefficients of two polynomials f and g in a polynomial ring is non-zero then the degree of the product of the polynomials is the sum of the degrees of f, g and the leading coefficient of the product fg is the product of the leading coefficients of f and g in that order. Thus, for each $A \in \mathcal{L}$, it is enough to give polynomials $p,\ q$ such that the leading coefficient of p or that of p^{-1} is in $\mathcal{L}$, the leading coefficient of q or that of q^{-1} is in $\mathcal{L}$ and the product of

leading coefficient of $p^{-1},\ q^{-1},\ p,\ q$ (in that order) is A. For the sake of simplicity we give polynomials of degree 1. Let

$$a = a(x) = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix},\ b = b(x) = \begin{pmatrix} x & -1+x \\ 1+x & x \end{pmatrix},$$
$$c = c(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ d = d(x) = \begin{pmatrix} x & 1 \\ -1+x & 1 \end{pmatrix},$$
$$e = e(x) = \begin{pmatrix} 1 & -1 \\ -x & 1+x \end{pmatrix},\ f = f(x) = \begin{pmatrix} x & 1+x \\ -1 & -1 \end{pmatrix},$$
$$g = g(x) = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix},\ h = h(x) = \begin{pmatrix} 1 & x \\ 1 & 1+x \end{pmatrix}.$$

Observe that each of these matrices is a unit in $M_2(R[x])$ such that either its leading coefficient or that of its inverse is in the set $\mathcal{L}$. Also, one can see that

$$(g,h) = \begin{pmatrix} x^3 & -1-x^2+x^3+x^4 \\ 1-x^2 & 1+2x-x^2-x^3 \end{pmatrix},$$
$$(c^{-1},d) = \begin{pmatrix} 1+x-2x^3+x^4 & x^3-x^2 \\ x^3-2x^2+x & 1-x+x^2 \end{pmatrix},$$
$$(a^{-1},b) = \begin{pmatrix} -1-2x-x^3+x^4 & -3x+2x^2-2x^3+x^4 \\ x+x^3 & -1+2x-x^2+x^3 \end{pmatrix},$$
$$(e,f) = \begin{pmatrix} 1+x+2x^2+2x^3+x^4 & 1+x+3x^2+3x^3+x^4 \\ 1+x^3+x^4 & 2-x+2x^3+x^4 \end{pmatrix},$$
$$(b^{-1},a) = \begin{pmatrix} -1+2x-2x^2-x^3+x^4 & -3x+x^3 \\ x-2x^2+x^4 & -1-2x+x^2+x^3 \end{pmatrix},$$
$$(b^{-1},a^{-1}) = \begin{pmatrix} -1+2x+x^2-x^3 & -x-2x^2+x^4 \\ 3x-x^3 & -1-2x-2x^2+x^3+x^4 \end{pmatrix}.$$

Note that the degree of each of these commutators is 4, the sum of the degrees of the polynomials involved and for each $A \in \mathcal{L}$, there is a commutator with leading coefficient A. □

With the notations of Proposition 4.1, write $\mathcal{L}^{-1} =$
$$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \right\}.$$
Observe that u is a unit in $M_2(R[x])$ with leading coefficient in the set $\mathcal{L}$ if and only if u^{-1} is a unit in $M_2(R[x])$ with leading coefficient in $\mathcal{L}^{-1}$. Also note that if (a,b) is a commutator, then $(a,b)^{-1}$ is also a commutator. Indeed, $(a,b)^{-1} = (b,a)$. Thus, by Proposition 4.1, for each $A \in \mathcal{L} \cup \mathcal{L}^{-1}$, the first derived subgroup of $M_2(R[x])$, has unit of degree 4 with leading coefficient A.

Corollary 4.2. *For any ring R and for any positive integer n, the n^{th} derived subgroup of the unit group of $M_2(R[x])$ has a unit with leading coefficient A for each A in the set $\mathcal{L}$ defined in Proposition 4.1.*

Proof. By Proposition 4.1, the first derived subgroup of $M_2(R[x])$ has units with degree 4 and the leading coefficient A for each $A \in \mathcal{L} \cup \mathcal{L}^{-1}$. Thus, the first derived subgroup of $M_2(R[x])$ has units, each of degree 4, having leading coefficients same as those of $a,\ b,\ c,\ d,\ e,\ f,\ g,\ h$ in the proof of Proposition 4.1. Thus, as in Proposition 4.1, we see that the second derived subgroup of $M_2(R[x])$ has units with degree 16 and leading coefficient A for each $A \in \mathcal{L} \cup \mathcal{L}^{-1}$. Repeated application of Proposition 4.1, now, gives the result. □

It follows from Corollary 4.2 that for every positive integer n, $\delta^{(n)}(\mathcal{U}(M_2(R[x]))) \neq I$. Hence we have the following corollary.

Corollary 4.3. *For any ring R, the unit group of $M_2(R[x])$ is not solvable.*

We now obtain conditions such that an element in $M_2(\mathbb{Z}_2[x])$ is a unit and use these conditions to give the form of units in $M_2(\mathbb{Z}_2[x])$. Note that units in $\mathbb{Z}_2[x]$ are precisely the units in $\mathbb{Z}_2$.

Theorem 4.4. *Any unit in $M_2(\mathbb{Z}_2[x])$ is of the form* $\begin{pmatrix} 1+x^ip(x) & x^jf(x) \\ x^kg(x) & 1+x^lq(x) \end{pmatrix}$ *where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_2[x]$, not necessarily non-zero, such that $p(x) + x^{l-i}q(x) + x^lp(x)q(x)$ is the product of $f(x)$, $g(x)$ and $i,\ j,\ k,\ l$ are non-negative integers such that $j + k = i$ and $1 \leq i \leq l$ or a matrix obtained from this form by a mere interchange of rows or columns or by an interchange of rows (columns) followed by an interchange of columns (rows).*

Proof. First observe that every matrix of the stated form is a unit under the stated condition. Now let $a = a(x)$, $b = b(x)$, $c = c(x)$, and $d = d(x)$ be polynomials in $\mathbb{Z}_2[x]$ such that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a unit in $M_2(\mathbb{Z}_2[x])$. Then the determinant of A is invertible in $\mathbb{Z}_2[x]$ and hence in $\mathbb{Z}_2$. Thus, the determinant of A is 1, that is, $ad - bc = 1$. Let $a = \sum_{i=0}^{m_1} a_ix^i,\ b = \sum_{j=0}^{m_2} b_jx^j,\ c = \sum_{k=0}^{l_1} c_kx^k$ and $d = \sum_{l=0}^{l_2} d_lx^l$. Since $ad - bc = 1$, we have $a_0d_0 - b_0c_0 = 1$. Thus, either $\{a_0d_0 = 1,\ b_0c_0 = 0\}$ or $\{a_0d_0 = 0,\ b_0c_0 = 1\}$. We will only consider the case when $a_0d_0 = 1$, $b_0c_0 = 0$, as units in the other case can be obtained by a mere interchange of rows/columns of units in the case $a_0d_0 = 1$, $b_0c_0 = 0$.

Since $a_0d_0 = 1$, we have $a_0 = d_0 = 1$. Thus, $a = 1 + x^ip(x)$ for some positive integer i and some polynomial $p(x) \in \mathbb{Z}_2[x]$, not necessarily non-zero, and $d = 1 + x^lq(x)$ for some positive integer l and some polynomial $q(x) \in \mathbb{Z}_2[x]$, not necessarily non-zero. Since $bc = ad - 1$, we have $bc = x^ip(x) + x^lq(x) + x^{i+l}p(x)q(x)$. Without any loss of generality, we can assume that $i \leq l$, for if $i > l$ then we can interchange the roles of a and d. Also then $b = x^jf(x)$, $c = x^kg(x)$ where $j + k = i$ and some polynomials $f(x),\ g(x) \in \mathbb{Z}_2[x]$ such that $p(x) + x^{l-i}q(x) + x^lp(x)q(x) = f(x)g(x)$. Hence $A = \begin{pmatrix} 1 + x^ip(x) & x^jf(x) \\ x^kg(x) & 1 + x^lq(x) \end{pmatrix}$ where $p(x), q(x), f(x), g(x) \in \mathbb{Z}_2[x]$ such that $p(x) + x^{l-i}q(x) + x^lp(x)q(x) = f(x)g(x)$ and $j,\ k$ are non-negative integers such that $j + k = i$.

Hence any unit in $M_2(\mathbb{Z}_2[x])$ is of the form $\begin{pmatrix} 1 + x^ip(x) & x^jf(x) \\ x^kg(x) & 1 + x^lq(x) \end{pmatrix}$ where $p(x), q(x), f(x), g(x) \in \mathbb{Z}_2[x]$, not necessarily non-zero, such that $p(x) + x^{l-i}q(x) + x^lp(x)q(x)$ is the product of $f(x), g(x)$, $1 \leq i \leq l$, and $j,\ k$ are non-negative integers such that $j + k = i$ or a matrix obtained from this form by a mere interchange of rows or columns or by an interchange of rows (columns) followed by interchange of columns (rows). □

We remark that the unit groups of $M_2(\mathbb{Z}_2[x])$ and $M_2(\mathbb{Z}_2)$ do not behave alike and have very different properties. Note that the unit group $\mathcal{U}(M_2(\mathbb{Z}_2))$, being isomorphic to S_3, is metabelian. The unit group $\mathcal{U}(M_2(\mathbb{Z}_2[x]))$ of $M_2(\mathbb{Z}_2[x])$ is, however, not even solvable (Corollary 4.3).

We now obtain conditions such that an element in $M_2(\mathbb{Z}_3[x])$ is a unit and use these conditions to give the form of units in $M_2(\mathbb{Z}_3[x])$. Once again we note that the units in $\mathbb{Z}_3[x]$ are precisely the units in $\mathbb{Z}_3$.

Theorem 4.5. *A unit in $M_2(\mathbb{Z}_3[x])$ is of one of the following forms:*

(1) $\begin{pmatrix} 1 + x^ip(x) & x^jf(x) \\ x^kg(x) & 1 + x^lq(x) \end{pmatrix}$ *where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $p(x) + x^{l-i}q(x) + x^lp(x)q(x)$ is the product of $f(x)$, $g(x)$ and $i,\ j,\ k,\ l$ are non-negative integers such that $j + k = i$, $1 \leq i \leq l$,*

(2) $\begin{pmatrix} 1 + x^ip(x) & x^jf(x) \\ x^kg(x) & -1 + x^lq(x) \end{pmatrix}$ *where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $-p(x) + x^{l-i}q(x) + x^lp(x)q(x)$ is the product*

of $f(x)$, $g(x)$ and $i,\ j,\ k,\ l$ are non-negative integers such that $j+k=i$, $1 \le i \le l$,

(3) $\begin{pmatrix} 1+x^i p(x) & 1+x^j m(x) \\ 1+x^k n(x) & -1+x^l q(x) \end{pmatrix}$ *where $p(x),\ q(x),\ m(x),\ n(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $1-x^i p(x)+x^l q(x)+x^{i+l}p(x)q(x)$ is the product of $1+x^j m(x)$, $1+x^k n(x)$ and $i,\ j,\ k,\ l$ are positive integers,*

or a matrix obtained from these forms by a mere interchange of rows or columns or by interchange of rows (columns) followed by interchange of columns (rows) or by taking their negatives or by interchanging rows (columns) followed by interchange of columns (rows) along with taking negatives.

Proof. Note that every matrix in any of the three stated forms is a unit under the stated condition. Now let $a = a(x)$, $b = b(x)$, $c = c(x)$, and $d = d(x)$ be polynomials in $\mathbb{Z}_3[x]$ such that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a unit in $M_2(\mathbb{Z}_3[x])$. Then the determinant of A is invertible in $\mathbb{Z}_3[x]$ and hence in $\mathbb{Z}_3$. Thus, the determinant of A is either 1 or -1. It is enough to consider only the case when determinant of A is 1, as units in the other case can be obtained by a mere interchange of rows or columns of the units in the case when determinant of A is 1. Let $a = \sum_{i=0}^{m_1} a_i x^i$, $b = \sum_{j=0}^{m_2} b_j x^j$, $c = \sum_{k=0}^{l_1} c_k x^k$ and $d = \sum_{l=0}^{l_2} d_l x^l$. Since $ad - bc = 1$, we have $a_0 d_0 - b_0 c_0 = 1$. Thus either $\{a_0 d_0 = 1,\ b_0 c_0 = 0\}$ or $\{a_0 d_0 = 0,\ b_0 c_0 = -1\}$ or $\{a_0 d_0 = -1,\ b_0 c_0 = 1\}$.

Case 1: $a_0 d_0 = 1$ and $b_0 c_0 = 0$. In this case, either $\{a_0 = d_0 = 1\}$ or $\{a_0 = d_0 = -1\}$.

If $a_0 = d_0 = 1$, then $a = 1 + x^i p(x)$ for some positive integer i and some polynomial $p(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, and $d = 1 + x^l q(x)$ for some positive integer l and some polynomial $q(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero. Since $bc = ad - 1$, we have $bc = x^i p(x) + x^l q(x) + x^{i+l} p(x)q(x)$. Without any loss of generality, we can assume that $i \le l$, for if $i > l$ then we can interchange the roles of a and d. Also then $b = x^j f(x)$, $c = x^k g(x)$ where $j + k = i$ and $p(x) + x^{l-i} q(x) + x^l p(x)q(x) = f(x)g(x)$. Hence $A = \begin{pmatrix} 1+x^i p(x) & x^j f(x) \\ x^k g(x) & 1+x^l q(x) \end{pmatrix}$ where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $p(x) + x^{l-i} q(x) + x^l p(x)q(x)$ is the product of $f(x)$, $g(x)$, $j + k = i$, $1 \le i \le l$.

If $a_0 = d_0 = -1$, then $a = -1 + x^i p(x)$ for some positive integer i and some polynomial $p(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, and $d = -1 + x^l q(x)$ for some positive integer l and some polynomial $q(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero. Since $bc = ad - 1$, we have $bc = -x^i p(x) - x^l q(x) + x^{i+l} p(x)q(x)$. Without any loss of

generality, we can assume that $i \leq l$, for if $i > l$ then we can interchange the roles of a and d. Also then $b = x^j f(x)$, $c = x^k g(x)$ where $j + k = i$ $-p(x) - x^{l-i}q(x) + x^l p(x)q(x) = f(x)g(x)$. Hence $A = \begin{pmatrix} -1 + x^i p(x) & x^j f(x) \\ x^k g(x) & -1 + x^l q(x) \end{pmatrix}$ where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $-p(x) - x^{l-i}q(x) + x^l p(x)q(x)$ is the product of $f(x)$, $g(x)$, $j + k = i$, $1 \leq i \leq l$. Observe that this matrix is of the same form as the negative of the matrix in the case $a_0 = d_0 = 1$.

Case 2: $a_0 d_0 = 0$ and $b_0 c_0 = -1$. In this case, either $\{b_0 = 1,\ c_0 = -1\}$ or $\{b_0 = -1,\ c_0 = 1\}$. If $b_0 = 1$ and $c_0 = -1$, then $b = 1 + x^j p(x)$ for some positive integer j and some polynomial $p(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, and $c = -1 + x^k q(x)$ for some positive integer k and some polynomial $q(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero. Since $ad = 1 + bc$, we have $ad = -x^j p(x) + x^k q(x) + x^{j+k} p(x)q(x)$. Without any loss of generality, we can assume that $j \leq k$, for if $j > k$ then we can interchange the roles of b and c. Hence, as earlier, $A = \begin{pmatrix} x^i f(x) & 1 + x^j p(x) \\ -1 + x^k q(x) & x^l g(x) \end{pmatrix}$ where $p(x),\ q(x),\ f(x),\ g(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $-p(x) + x^{k-j}q(x) + x^k p(x)q(x)$ is the product of $f(x)$, $g(x)$, $i + l = j$, $1 \leq j \leq k$. Note that units of this form can be obtained from the form (2) by the interchange of columns.

If $b_0 = -1$ and $c_0 = 1$, then, as in Case 1, units in this subcase have the form that can be obtained from the forms in the subcase $b_0 = 1, c_0 = -1$ by simply taking the negative of the matrix.

Case 3: $a_0 d_0 = -1$ and $b_0 c_0 = 1$. In this case, either $\{a_0 = 1,\ d_0 = -1,\ b_0 = 1,\ c_0 = 1\}$ or $\{a_0 = 1,\ d_0 = -1,\ b_0 = -1,\ c_0 = -1\}$ or $\{a_0 = -1,\ d_0 = 1,\ b_0 = 1,\ c_0 = 1\}$ or $\{a_0 = -1,\ d_0 = 1,\ b_0 = -1,\ c_0 = -1\}$. If $\{a_0 = 1,\ d_0 = -1,\ b_0 = 1,\ c_0 = 1\}$, then $a = 1 + x^i p(x)$ for some positive integer i and some polynomial $p(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, $d = -1 + x^l q(x)$ for some positive integer l and some polynomial $q(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, $b = 1 + x^j m(x)$ for some positive integer j and some polynomial $m(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, and $c = 1 + x^k n(x)$ for some positive integer k and some polynomial $n(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero. Since $bc = ad - 1$, we have $1 - x^i p(x) + x^l q(x) + x^{i+l} p(x)q(x) = (1 + x^j m(x))(1 + x^k n(x))$. Hence $A = \begin{pmatrix} 1 + x^i p(x) & 1 + x^j m(x) \\ 1 + x^k n(x) & -1 + x^l q(x) \end{pmatrix}$ where $p(x),\ q(x),\ m(x),\ n(x) \in \mathbb{Z}_3[x]$, not necessarily non-zero, such that $1 - x^i p(x) + x^l q(x) + x^{i+l} p(x)q(x)$ is the product of $1 + x^j m(x)$, $1 + x^k n(x)$ and $i,\ j,\ k,\ l$ are positive integers.

It can be seen that the form of units in the remaining subcases can be obtained from the units in the subcase $\{a_0 = 1,\ d_0 = -1,\ b_0 = 1,\ c_0 = 1\}$ by interchanging rows (columns) followed by columns (rows) or by taking their negatives or by interchanging rows (columns) followed by columns (rows) along with taking negatives. □

In this case also we remark that the unit group of $M_2(\mathbb{Z}_3[x])$ and that of $M_2(\mathbb{Z}_3)$ do not behave alike and have different properties. In fact, if $V = \mathcal{U}(M_2(\mathbb{Z}_3)) = GL(2, \mathbb{Z}_3)$, then V is solvable of length 4 as $V \cong GL(2, \mathbb{Z}_3)$, $\delta^1(V) \cong SL(2, \mathbb{Z}_3)$, $\delta^3(V) \cong C_2$, therefore $\delta^4(V) = (1)$. However, the unit group $\mathcal{U}(M_2(\mathbb{Z}_3[x]))$ is not solvable by Corollary 4.3.

References

[1] P. B. Bhattacharya and S. K. Jain, *A note on the adjoint group of a ring*, Arch. Math. (Basel), 21 (1970), 366-368.

[2] P. B. Bhattacharya and S. K. Jain, *Rings having solvable adjoint groups*, Proc. Amer. Math. Soc., 25 (1970), 563-565.

[3] V. Bovdi and M. Salim, *On the unit group of a commutative group ring*, Acta Sci. Math. (Szeged), 80(3-4) (2014), 433-445.

[4] D. M. Burton, Elementary Number Theory, McGraw-Hill Education, 7th edition, 2011.

[5] J. L. Fisher, M. M. Parmenter and S. K. Sehgal, *Group rings with solvable n-Engel unit groups*, Proc. Amer. Math. Soc., 59(2) (1976), 195-200.

[6] K. R. Goodearl, Von Neumann Regular Rings, Second edition, Robert E. Krieger Publishing Co., Inc., Malabar, FL, 1991.

[7] P. Kanwar, A. Leroy and J. Matczuk, *Idempotents in ring extensions*, J. Algebra, 389 (2013), 128-136.

[8] P. Kanwar, A. Leroy and J. Matczuk, *Clean elements in polynomial rings*, Noncommutative Rings and their Applications, Contemp. Math., Amer. Math. Soc., 634 (2015), 197-204.

[9] P. Kanwar, R. K. Sharma and P. Yadav, *Lie regular generators of general linear groups II*, Int. Electron. J. Algebra, 13 (2013), 91-108.

[10] C. Lanski, *Some remarks on rings with solvable units*, Ring Theory, (Proc. Conf., Park City, Utah, 1971), Academic Press, New York, (1972), 235-240.

[11] B. R. McDonald, Linear Algebra over Commutative Rings, Monographs and Textbooks in Pure and Applied Mathematics, 87, Marcel Dekker, Inc., New York, 1984.

[12] M. Mirowicz, *Units in group rings of the infinite dihedral group*, Canad. Math. Bull., 34(1) (1991), 83-89.

[13] W. K. Nicholson, *Lifting idempotents and exchange rings*, Trans. Amer. Math. Soc., 229 (1977), 269-278.

[14] W. K. Nicholson, *Strongly clean rings and Fitting's lemma*, Comm. Algebra, 27(8) (1999), 3583-3592.

[15] R. K. Sharma, P. Yadav and P. Kanwar, *Lie regular generators of general linear groups*, Comm. Algebra, 40(4) (2012), 1304-1315.

[16] L. Wiechecki, *Group algebra units and tree actions*, J. Algebra, 311(2) (2007), 781-799.

Pramod Kanwar (Corresponding Author)
Department of Mathematics
Ohio University-Zanesville
Zanesville, Ohio, USA
e-mail: kanwar@ohio.edu

Meenu Khatkar and **R. K. Sharma**
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi, 110016, India
e-mails: meenukhatkar@gmail.com (M. Khatkar)
rksharmaiitd@gmail.com (R. K. Sharma)