THE CONJUGACY PROBLEM FOR TWO-BY-TWO MATRICES OVER POLYNOMIAL RINGS

F. J. Grunewald and N. K. Iyudu

ABSTRACT. We give an effective solution of the conjugacy problem for two-by-two matrices over the polynomial ring in one variable over a finite field.

CONTENTS

1. Introduction ............................................................................................................. 2233
2. Reduction to a Quadratic Equation ........................................................................ 2234
3. Preliminary Considerations for the Solution of the Quadratic Equation .......... 2236
4. Imaginary Case ....................................................................................................... 2238
5. Real Case ................................................................................................................ 2239
   5.1. Units (equation $u^2 + bvu + cv^2 = 1$) ......................................................... 2239
   5.2. General Case $d \neq 1$ .................................................................................... 2242
6. Note on the Case of Characteristic Not Equal to 2 ............................................. 2244
7. Centralizers of Matrices ....................................................................................... 2246
8. The Conjugacy Problem in $GL(2)$ over Polynomial Rings ............................ 2246
   References .............................................................................................................. 2247

1. Introduction

We consider the conjugacy problem in the ring of two-by-two matrices $M(2, k[x])$ over the polynomial ring $k[x]$, where $k$ is a finite field. We say that two matrices $A, B \in M(2, k[x])$ are conjugate if there is a conjugating matrix $U$ in the group $GL(2, k[x])$ of invertible matrices over $k[x]$, i.e., $U$ satisfies $B = UAU^{-1}$. In what follows, we write $\deg(P)$ for the degree of a polynomial and $\deg(A)$ for the maximal degree of the entries of $A \in M(2, k[x]).$

Theorem 1.1. Let $k$ be a finite field with $q$ elements and $A, B \in M(2, k[x])$. Let $\delta$ be the maximum of $\deg(A)$ and $\deg(B)$. If $A$ and $B$ are conjugate, then there is a conjugating matrix $U$ with $\deg(U) \leq (1 + q)\delta q^{78}$.

For certain pairs of matrices $A, B \in M(2, k[x])$, the estimate of the degrees of the entries of $U$ can be improved to be linear in $\delta$ independently of $q$ (see Proposition 4.2). Theorem 1.1 shows that there is an algorithm that decides whether two matrices $A, B \in M(2, k[x])$ are conjugate or not. Hence we can state the following corollary.

Corollary 1.2. Let $k$ be a finite field. Then the conjugacy problem in the group $GL(2, k[x])$ is effectively solvable.

Corollary 1.2 should be compared with the solution of the conjugacy problem in an arithmetic group. The conjugacy problem for $GL(n, k)$ ($n \in \mathbb{N}$) was solved in [4]. But even for the case $n = 2$ no explicit estimates like those that follow from Theorem 1.1 are known. Also, the algorithms described in [5], which solve the conjugacy problem in any arithmetic group, do not give estimates for the size of a conjugating matrix.
matrix. The method of solution employed in [4] for the case of \( \text{GL}(n, \mathbb{Z}) \) (where \( n \in \mathbb{N} \) can be extended (without giving estimates) to the case of \( \text{GL}(n, k[x]) \) (where \( n \in \mathbb{N} \) and \( k \) is a finite field), where the characteristic of the field \( k \) does not divide the size \( n \) of the matrices. Also, our method provides extra difficulties in the case where \( k \) has characteristic 2. Further features of the conjugacy problem in \( \text{GL}(2, k[x]) \) are described in Sec. 8.

Given a matrix \( A \in \text{GL}(2, k[x]) \), we define

\[
Z(A) := \{ U \in \text{GL}(2, k[x]) \mid UAU^{-1} = A \}
\]

(1)

to be its centralizer. In the case where \( A \neq 1 \) is semisimple, it is well known that \( Z(A) \) is either finite or the direct product of an infinite cyclic group and a finite group (see Sec. 7). By our methods we can give an estimate for the degrees of the entries of a generator of the infinite part.

**Theorem 1.3.** Let \( k \) be a finite field with \( q \) elements and \( A \in \text{GL}(2, k[x]) \) be a semisimple matrix not equal to the identity matrix. Let \( Z(A) \) be infinite. Then there is a matrix \( U \in Z(A) \) that generates \( Z(A) \) up to a finite group with \( \deg(U) \leq \deg(A) q^{2 \deg(A)} \).

Our method to prove Theorem 1.1 uses a reduction to a quadratic equation in two variables. As a special case, Pell’s equation

\[
u^2 + Dv^2 = 1
\]

(2)

with \( D \in k[x] \) arises. Let us call \( D \in k[x] \) positive if it is neither constant nor a square, \( D \) has an even degree, and its highest coefficient is a square. Let us furthermore call a solution \((u, v)\) of (2) trivial if \( u, v \in k \) holds.

**Theorem 1.4.** Let \( k \) be a finite field with \( q \) elements and \( D \in k[x] \) be a positive polynomial. Then (2) has a nontrivial solution \((u, v)\in k^2\) with \( \deg(u), \deg(v) \leq q^{\deg(D)} \).

Pell’s equation (2) has been studied extensively in the paper of Emil Artin of 1924 [2]. He investigates Pell’s equation through continued-fraction expansions. But he has to assume that the characteristic of \( k \) is not equal to 2. Our result in Theorem 1.4 follows straightforwardly from [2]. We modify Artin’s technique for the case of characteristic 2.

Following our reduction, we have to analyze the solutions of general quadratic equations

\[
a u^2 + b u v + c v^2 = d,
\]

(3)

where \( a, b, c, \) and \( d \) are polynomials in \( k[x] \). In the case where the characteristic of \( k \) is not 2, appropriate results can be deduced by the continued-fraction methods of [2]. In the case where the characteristic of \( k \) is 2, we use new degree functions on certain quadratic extension rings of \( k[x] \) to control the behavior of continued-fraction expansions.

2. Reduction to a Quadratic Equation

Let \( k \) be a field. Here we consider pairs of matrices

\[
A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M(2, k[x]), \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M(2, k[x]),
\]

(4)

which we call rationally conjugate if they are conjugate by an element of \( \text{GL}(2, k(x)) \), where \( k(x) \) is the field of rational functions over \( k \). Being rationally conjugate is equivalent to the conditions

\[
\text{Tr}(A) = \text{Tr}(B), \quad \det(A) = \det(B),
\]

(5)

where \( \text{Tr}(A) \) denotes the trace and \( \det(A) \) denotes the determinant of the matrix \( A \).

Suppose we want to find a matrix

\[
U = \begin{pmatrix} u & p \\ v & q \end{pmatrix} \in \text{GL}(2, k[x])
\]

(6)