Generalized Inverses of Matrices of Skew Polynomials

by

Weixi Gu

A Thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfilment of the requirements of the degree of

MASTER OF SCIENCE

Department of Mathematics

University of Manitoba

Winnipeg

Abstract

Generalized inverses of matrices are of great importance in the resolution of linear systems and have been extensively studied by many researchers. A collection of some results on generalized inverses of matrices over commutative rings has been provided by K. P. S. Bhaskara Rao [30]. In this thesis, we consider constructing algorithms for finding generalized inverses and generalizing the results collected in [30] to the non-commutative case.

We first construct an algorithm by using the greatest common divisor to find a generalized inverse of a given matrix over a commutative Euclidean domain. We then build an algorithm for finding a generalized inverse of a matrix over a non-commutative Euclidean domain by using the one-sided greatest common divisor and the least common left multiple. Finally, we explore properties of various generalized inverses including the Moore-Penrose inverse, the group inverse and the Drazin inverse in the non-commutative case.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my advisors, Prof. Yang Zhang and Prof. Guenter Krause, whose research knowledge and gentle encouragement helped me throughout the period of my research work and the writing of this thesis. I am also grateful to the members of my thesis committee who provided constructive comments on my research. I would like to thank Prof. Yang Zhang, the Department of Mathematics, the Faculty of Graduate Studies and the Faculty of Science of the University of Manitoba, for the financial support of my graduate study. As well, I thank my friends in the department of mathematics for their support and encouragement. Finally, I am deeply grateful to my family who supported my decision to pursue a higher education and encouraged me through my life to do the best I can.

Contents

Notation and Terminology

Below is a list of special notation and terminology to be used in Chapters 1 to 4. (Notation that is either standard or only used locally has not been included.)

$\mathbb{F}$	a field
R	a division ring, p. 10
σ	an automorphism of R, p. 10
σ^{-1}	the inverse of σ
δ	a σ-derivation, p. 2
$\sigma\delta$ ($\delta\sigma$, resp.)	the composite mapping $\sigma \circ \delta$ ($\delta \circ \sigma$, resp.)
S	the skew polynomial ring $R[x; \sigma, \delta]$, p. 10
$Q(S)$	the Ore quotient ring of S, p. 14
$\mathrm{lc}(f)$	the leading coefficient of a polynomial f in S, p. 1.2
$\mathrm{nf}(f)$	the normal form of a polynomial f in S, p. 1.2
$a \,\mathrm{quo}_\mathrm{l}\, b$ ($a \,\mathrm{quo}_\mathrm{r}\, b$)	the left (right) quotient of the division of a by b, p. 11
$\underline{0}$	a zero matrix of suitable size
$A(i,j)$	the $(i,j)^{th}$ entry of a matrix A
$(a_{ij})_{m\times n}$	an $m \times n$ matrix in which the $(i,j)^{th}$ entry is a_{ij}
$\det(A)$	the determinant of a matrix A over a commutative ring
$\mathrm{adj}(A)$	the adjoint matrix of a matrix A over a commutative ring

$\mathrm{Row}_i(A)$	the ith row of a matrix A ($i \in \mathbb{N}$), p. 28
$\mathrm{Col}_i(A)$	the ith column of a matrix A ($i \in \mathbb{N}$), p. 28
Ro	a unimodular matrix corresponding to row operations, p. 27
Co	a unimodular matrix corresponding to column operations, p. 28
A^*	the involution transpose of a matrix A, p. 5
A^-	a $\{1\}$-inverse of a matrix A, p. 6
A^+	the Moore-Penrose inverse of a matrix A, p. 7
$A^\#$	the group inverse of a matrix A, p. 7
$\mathrm{rank}(M)$	the (unique) rank of a free module M, p. 17
$\rho(A)$	the (inner) rank of a matrix A, p. 19
$\mathrm{diag}(A, B)$	$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$, where A, B are matrices, p. 19
$Z(P)$	the center of a ring P, p. 48
$\mathbb{M}_{m\times n}(P)$	the ring of all $m \times n$ matrices over P
$\mathbb{M}_m(P)$	the ring of all $m \times m$ matrices over P
$\oplus$	direct sum of modules
$\otimes$	tensor product of modules
$A \leftarrow B$	assign a value B to a variable A, p. 27
$\begin{bmatrix} \end{bmatrix}$	an empty matrix, p. 28

Introduction

Generalized Inverses

A generalized inverse of a matrix A, as the name implies, is a matrix G that is analogous to the usual inverse, and it possibly exists when A is singular or even rectangular. In other words, given a matrix A, a generalized inverse of A is a matrix G such that

$$AGA = A. \tag{1}$$

If A is a square nonsingular matrix, then G reduces to the usual inverse of A.

The theory of the generalized inverse for matrices originated from the need of finding a solution to a linear system of algebraic equations. Concretely, the concept of a generalized inverse was first introduced in 1903 by Fredholm [12], where a particular generalized inverse that serves as an integral operator was called "pseudoinverse". The notion of a generalized inverse for a matrix (not necessarily a square matrix) was mentioned for the first time by Moore [25] in 1920. However, in the following 30 years, except for a few extensions of Moore's work, no systematic study was done on the subject due to the ambiguous notion.

The first breakthrough in the study of generalized inverses came in 1955, when Penrose [28] redefined the Moore generalized inverse based on the results obtained by Bjerhammar ([1], [2]) in 1951. In his paper, Penrose introduced a generalized inverse satisfying the four equations (1.1)-(1.4) in Chapter 1, and showed the uniqueness of the inverse. This discovery has greatly affected and promoted the

development of the theory of generalized inverses, and the generalized inverse defined by Penrose is therefore widely known as the *Moore-Penrose inverse*.

Today, the literature on the theory of generalized inverses is extensive. A variety of generalized inverses, such as the group inverse and the Drazin inverse, have been constructed for different purposes. To avoid confusion, we shall refer to the generalized inverse satisfying condition (1) as {1}-inverse for the rest of this thesis.

The application of generalized inverses of matrices has been extended to several areas, including statistics, numerical analysis, and cryptography. For example, the Moore-Penrose inverse is commonly used to find a least square solution to a linear system that has multiple solutions (Penrose and Todd [29]) and to solve problems in linear statistical models (Kirkland [19]); the Drazin inverse plays an important role in singular linear systems, differential equations and Markov chains (Hanke [15], Campbell [6], C. D. Meyer, Jr [22, 23]); generalized inverses of matrices over finite fields have been proposed as protential tools in cryptographic research (Wu [32, 33]).

To analyze the properties of generalized inverses of matrices, many algorithms have been proposed. For instance, K. P. S. B. Rao [30] has introduced an algorithm for determining the existence of a generalized inverse and finding a generalized inverse of a given matrix over a commutative principal ideal domain; Courrieu [11], Katsikis and Pappas ([17] [18]) have introduced fast algorithms for computing Moore-Penrose inverses of real matrices; Miljković [24] has introduced iterative methods for computing generalized inverses of complex matrices. Nevertheless, fast algorithms for finding generalized inverses of matrices, especially in the non-commutative case, are still in great demand.

Skew Polynomial Rings

A skew polynomial ring, also called an Ore extension, is a polynomial ring whose multiplication by the indeterminate is "skewed" by an endomorphism and an

associated skew derivation on the coefficient ring. Concretely, let R be a ring, σ a ring endomorphism of R, and let δ be a σ-derivation on R, namely, an additive map $\delta : R \to R$ satisfying $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in R$. A *skew polynomial ring over* R, written $S = R[x; \sigma, \delta]$, is a ring S satisfying the following conditions:

(a) S is a ring, containing R as a subring;

(b) x is an element of S;

(c) S is a free left R-module with basis $\{1, x, x^2, ...\}$;

(d) $xr = \sigma(r)x + \delta(r)$ for all $r \in R$.

For any element f of S, f is uniquely expressed in the form

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $n \in \mathbb{N}$ and $a_0, ..., a_n \in R$. If R is a commutative ring, σ is the identity mapping and δ is the zero derivation, then the skew polynomial ring S reduces to the ordinary polynomial ring $R[x]$.

The concept of a skew polynomial ring was first considered in 1920 by Noether and Schmeidler [26]. In 1933, the general definition of a skew polynomial ring was introduced by Ore [27], who first systematically studied this object. Since then, the structure and construction of skew polynomial rings have been extensively studied by numerous authors, such as Jacobson [16], Cohn [9], and Lam [21], and the theory of skew polynomials has thus had a substantial growth.

It has been shown that the study of skew polynomial rings is of great importance and has applications in many research areas. In pure mathematics, skew polynomials can be used for solving systems of linear differential and difference equations (Bronstein and Petkovšek [5]). In coding theory, skew polynomial rings over finite fields can be used to study linear codes and to construct error-correcting

codes (Boucher, [3], [4]). In control theory, linear control systems over Ore algebras have been investigated for potential values and applications in electrical engineering and computer science (Chyzak, Quadrat and Robertz [7]).

Outline of the Thesis

This thesis is organized as follows.

In Chapter 1, we outline the basic definitions and results to be used in the thesis.

In Chapter 2, we construct an algorithm for finding {1}-inverses of matrices over commutative Euclidean domains by using the extended Euclidean algorithm and some properties of the greatest common divisor. Given a matrix A, the algorithm first determines the existence of a {1}-inverse of A, then computes a {1}-inverse of A (if there is any). The complexity of the algorithm is given for comparing its efficiency with that of others. Some examples are presented for the demonstration of the algorithm.

In Chapter 3, we build an algorithm for finding {1}-inverses of matrices over a skew polynomial ring S (whose definition is given in Chapter 1) based on the fact that S is a non-commutative Euclidean domain. Compared with the algorithm in Chapter 2, this algorithm is constructed by using one-sided greatest common divisors and least common multiples.

In Chapter 4, we investigate the existence and construction of various generalized inverses of matrices including {1}-inverses, Moore-Penrose inverses and Drazin inverses.

In the Appendix, we give the Maple codes of the first algorithm.

Chapter 1

Preliminaries

This chapter outlines some of the basic mathematical definitions and results relevant to the thesis.

1.1 Generalized Inverses for Matrices

It is known that there are different types of generalized inverses for matrices. In this section, we list the definitions and properties of the generalized inverses to be investigated in this thesis.

Let P be a ring. An *involution* on P is an anti-automorphism f on P of order 2. The image of an element $p \in P$ under f, written $\overline{p}$, is called *the involution of* p. We define a mapping $g : \mathbb{M}_{m\times n}(P) \to \mathbb{M}_{n\times m}(P)$ such that for $A = (a_{ij}) \in \mathbb{M}_{m\times n}(P)$, $g(A) = A^*$, where $A^* = (\overline{A})^T$, $\overline{A} = (\overline{a_{ij}})_{m\times n}$. We call the image A^* of the matrix A under the mapping g the *involution transpose* of A. By definition, we have

$$(A^*)^* = A,$$
$$(AB)^* = B^*A^*.$$

For this section, we now fix the notation that P is a ring (not necessarily

commutative) with an involution, $A_{m\times n}$, $G_{n\times m}$ $(m, n \in \mathbb{N})$ are two matrices over P and $k \in \mathbb{Z}^+$. Consider the following equations.

$$AGA = A \tag{1.1}$$

$$GAG = G \tag{1.2}$$

$$(AG)^* = AG \tag{1.3}$$

$$(GA)^* = GA \tag{1.4}$$

$$AG = GA \tag{1.5}$$

$$A^k = A^{k+1}G. \tag{1.6}$$

Definition 1.1. *(a) If A and G satisfy Equation (1.1), then G is called a $\{1\}$-inverse of A, written A^-, over P. If A has a $\{1\}$-inverse, then A is called a regular matrix. The matrix ring $\mathbb{M}_{n\times n}(P)$ $(n \in \mathbb{N})$ is called a regular ring if every matrix from $\mathbb{M}_{n\times n}(P)$ is regular.*

(b) If A and G satisfy Equation (1.1) and (1.2), then G is called a $\{1, 2\}$-inverse of A over P. Generalized inverses named $\{1, 2, 3\}$-inverse, $\{1, 2, 4\}$-inverse and so on are defined analogously.

Proposition 1.1. *A $\{1\}$-inverse for a matrix is not unique.*

If G is a $\{1\}$-inverse of A, then GAG is a $\{1\}$-inverse of A. For example, let $A = \begin{bmatrix} 3x+1 & 2x & 1 \\ 0 & x^2 & x+1 \end{bmatrix}$ be a matrix over the polynomial ring $\mathbb{Q}[x]$. Then $G = \begin{bmatrix} 1-\frac{3}{2}x^2-\frac{3}{5}x^3 & -1-\frac{2}{5}x \\ -\frac{3}{2}+\frac{33}{10}x^2+\frac{9}{5}x^3 & \frac{11}{5}+\frac{6}{5}x \\ -\frac{9}{5}x^4-\frac{3}{2}x^3+\frac{3}{2}x^2 & -\frac{6}{5}x^2-x+1 \end{bmatrix}$ is a $\{1\}$-inverse of A. One can verify that $GAG = \begin{bmatrix} 1-\frac{3}{2}x^2-\frac{3}{5}x^3 & -1-\frac{2}{5}x \\ -\frac{3}{2}+\frac{33}{10}x^2+\frac{9}{5}x^3 & \frac{11}{5}+\frac{6}{5}x \\ -\frac{9}{5}x^4-\frac{3}{2}x^3+\frac{3}{2}x^2 & -\frac{6}{5}x^2-x+1 \end{bmatrix}$ is also a $\{1\}$-inverse of A.

Proposition 1.2. *If A has a $\{1\}$-inverse over P, then A has a $\{1, 2\}$-inverse*

over P.

If G_1 and G_2 are two $\{1\}$-inverses of A over P, then G_1AG_2 is a $\{1,2\}$-inverse of A over P.

Proposition 1.3. *If A has a $\{1,3\}$-inverse over P, then A has a $\{1,2,3\}$-inverse over P.*

If G is a $\{1,3\}$-inverse of A, then GAG is a $\{1,2,3\}$-inverse of A.

Definition 1.2. *If A and G satisfy Equations (1.1) to (1.4), then G is called the Moore-Penrose inverse (MP-inverse, for short) of A, written A^+, over P.*

Lemma 1.1. *([30], p16) The MP-inverse of a matrix is unique.*

Note that if A has a $\{1,3\}$-inverse G_1 and a $\{1,4\}$-inverse G_2 over P, then G_2AG_1 is a MP-inverse of A over P.

Proposition 1.4. *([30], Proposition 3.10)*

(a) $A_{m\times n}$ has a $\{1,3\}$-inverse if and only if (i) A^*A is regular and (ii) for a matrix $C_{n\times s}$ ($s \in \mathbb{N}$) over P, $AC = 0$ whenever $A^*AC = 0$.

(b) $A_{m\times n}$ has a $\{1,4\}$-inverse if and only if (i) AA^* is regular and (ii) for a matrix $D_{k\times s}$ ($s \in \mathbb{N}$), $DA = 0$ whenever $DAA^* = 0$.

(c) $A_{m\times n}$ has an MP-inverse if and only if (i) A^*A and AA^* are both regular and (ii) for any matrices $C_{n\times s}$ and $D_{t\times m}$ over P ($s,t \in \mathbb{N}$), $AC = 0$ whenever $A^*AC = 0$ and $DA = 0$ whenever $DAA^* = 0$.

(d) $A_{m\times n}$ has an MP inverse if and only if (i)A^*AA^* is regular and (ii) A has the properties that, for any matrices $C_{n\times s}$ and $D_{t\times m}$ over P ($s,t \in \mathbb{N}$), $AC = 0$ whenever $A^*AC = 0$ and $DA = 0$ whenever $DAA^* = 0$.

Definition 1.3. *(a) If A and G satisfy Equations (1.1) and (1.5), then G is called a commuting g-inverse of A over P.*

(b) If A and G satisfy Equations (1.1), (1.2) and (1.5), then G is called a group inverse of A, written $A^{\#}$, over P.

(c) If A and G satisfy Equations (1.2), (1.5) and (1.6), then G is called a Drazin inverse of A over P.

From the definitions we can see that the Drazin inverse is a generalization of the group inverse.

Proposition 1.5. *([30], p. 89) The group inverse of a matrix is unique.*

Proposition 1.6. *([30], Proposition 6.23) The Drazin inverse of a matrix is unique.*

1.2 General Skew Polynomial Rings

In the Introduction, we saw that the indeterminate of a skew polynomial does not commute with its coefficients. In order to work with skew polynomial computations, we introduce the Leibniz rule for skew polynomial multiplication and rules for exchanging the indeterminate and coefficients of a skew polynomial in this section.

Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring and $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in S$ with $a_0, a_1, ..., a_n \in R$, $a_n \neq 0$. The *degree* of f, written $\deg(f)$, is defined to be $\max\{i | a_i \neq 0,\ i = 0, 1, ..., n\}$. The *leading coefficient* of f, written $\mathrm{lc}(f)$, is defined to be a_n. If $f = 0$, then $\deg(f) = -\infty$, $\mathrm{lc}(f) = 0$. If the coefficient ring R is a skew field, then we define the *normal form* of f, written $\mathrm{nf}(f)$, to be $(\mathrm{lc}(f))^{-1} f$. For any two skew polynomials f_1 and f_2 in S, the degrees of their sum and product satisfy the following condition:

$$\deg(f_1 + f_2) \leq \max\{\deg(f_1),\ \deg(f_2)\}.$$

Moreover, if the coefficient ring R is a domain, then

$$\deg(f_1 f_2) = \deg(f_1) + \deg(f_2).$$

Lemma 1.2. *(Leibniz rule) Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring. For any $r \in S$,*

$$x^k r = \sum_{i=0}^{k} \binom{k}{i} \sigma^i \delta^{k-i}(r) x^i. \tag{1.7}$$

If $\sigma = 1,\ \delta \neq 0$, then

$$x^k r = \sum_{i=0}^{k} \binom{k}{i} \delta^{k-i}(r) x^i, \quad r x^k = \sum_{i=0}^{k} \binom{k}{i} (-1)^{k-i} x^i \delta^{k-i}(r); \tag{1.8}$$

if $\sigma \neq 1,\ \delta = 0$, then

$$x^k r = \sigma^k(r) x^k, \quad r x^k = x^k \sigma^{-k}(r). \tag{1.9}$$

The above rule can be shown by induction. Clearly, (1.7) holds for $k = 1$. Suppose (1.7) holds for all $k = n$ where $n \in \mathbb{N},\ n \geq 1$. Then for $k = n + 1$, we have

$$\begin{aligned}
x^k r &= x \left(\sum_{i=0}^{n} \binom{n}{i} \sigma^i \delta^{n-i}(r) x^i \right) \\
&= \sum_{i=0}^{n} \binom{n}{i} x \sigma^i \delta^{n-i}(r) x^i \\
&= \sum_{i=0}^{n} \binom{n}{i} \left(\sigma^{i+1} \delta^{n-i}(r) x^{i+1} + \sigma^i \delta^{n-i+1}(r) x^i \right) \\
&= \binom{n}{0} \left(\sigma \delta^n(r) x + \delta^{n+1}(r) \right) + \cdots + \binom{n}{n} \left(\sigma^{n+1} x^{n+1} + \sigma^n \delta(r) x^n \right) \\
&= \binom{n}{0} \delta^{n+1}(r) + \sum_{i=1}^{n} \left(\binom{n}{i-1} + \binom{n}{i} \right) \sigma^i \delta^{n-i+1}(r) x^i + \binom{n}{n} \sigma^{n+1}(r) x^{n+1} \\
&= \binom{n+1}{0} \delta^{n+1}(r) + \sum_{i=1}^{n} \binom{n+1}{i} \sigma^i \delta^{n-i+1}(r) x^i + \binom{n+1}{n+1} \sigma^{n+1}(r) x^{n+1}
\end{aligned}$$

$$= \sum_{i=0}^{n+1} \binom{n+1}{i} \sigma^i \delta^{n+1-i}(r) x^i$$
$$= \sum_{i=0}^{k} \binom{k}{i} \sigma^i \delta^{k-i}(r) x^i.$$

Thus, (1.7) holds for all $r \in R$. Identities (1.8) and (1.9) follow directly from (1.7).

Lemma 1.3. *Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring. For any $r, s \in R$, $k \in \mathbb{N}$,*

$$\delta^k(rs) = \sum_{i=0}^{k} \binom{k}{i} \sigma^{k-i} \delta^i(r) \delta^{k-i}(s). \tag{1.10}$$

Lemma 1.4. *Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring. Let $k \geq 1$ be an integer. If $\delta = 0$, then for any $a \in R$,*

$$(xa)^k = x^k \left(\prod_{i=1}^{k} \sigma^{-k+i}(a) \right) = \left(\prod_{i=1}^{k} \sigma^i(a) \right) x^k. \tag{1.11}$$
$$(ax)^k = x^k \left(\prod_{i=0}^{k-1} \sigma^{-k+i}(a) \right) = \left(\prod_{i=0}^{k-1} \sigma^i(a) \right) x^k. \tag{1.12}$$

1.3 A Skew Polynomial Ring S

From now on, we fix the notation that $S = R[x; \sigma, \delta]$ is a skew polynomial ring, where R is a division ring, σ is an automorphism of R and δ is a σ-derivation. We shall give conditions for S to be a (non-commutative) Euclidean domain and an Ore domain (and thus to have a unique ring of fractions) in order to support the investigation on generalized inverses of matrices over S in Chapters 3 and 4 of this thesis.

1.3.1 Euclidean Domains

Recall that a *principal left (right, resp.) ideal domain* is a domain in which every left (right, resp.) ideal is generated by a single element, and a principal left and

right ideal domain is called a *principal ideal domain* (PID).

Proposition 1.7. *([14], Theorem 2.8) The skew polynomial ring S is a PID.*

We now turn to Euclidean domains. A *left (right, resp.) Euclidean domain* is a domain D with a function $d: D \to \mathbb{N} \bigcup \{-\infty\}$ such that for all $a, b \in D$ with $b \neq 0$, there exist $q, r \in D$ such that

$$a = qb + r \ (a = bq + r, \text{ resp.}), \ d(r) < d(b),$$

in other words, for any $a, b \in D$ with $b \neq 0$, $d(a) \geq d(b)$, there exists $c \in D$ satisfying

$$d(a - cb) < d(a) \ (d(a - bc) < d(a), \text{ resp.}). \tag{1.13}$$

The element q is called the *left (right, resp.) quotient* of the division of a by b, written $q = a \operatorname{quo_l} b$, ($q = a \operatorname{quo_r} b$, resp.). The function d is called a *left (right, resp.) Euclidean function* on D. A ring that is a left and right Euclidean domain is simply called a *Euclidean domain*.

Proposition 1.8. *Let $d: S \to \mathbb{N} \bigcup \{-\infty\}$ denote the degree function over S. Then S is a Euclidean domain with d being a Euclidean function on it.*

The above proposition can be shown as follows. Let $f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$ be polynomials in S such that $g_m \neq 0$. By (1.13), it suffices to show that

$$\text{there exist } h_1, h_2 \in S \text{ such that } d(f - h_1 g) < d(f), \ d(f - g h_2) < d(f). \tag{1.14}$$

If $d(f) < d(g)$, then (1.14) is clear. Suppose $d(f) \geq d(g)$. Then $f_n \neq 0$. Since σ is an automorphism of R and $g_m \neq 0$, we have $\sigma^{n-m}(g_m) \in R \setminus \{0\}$, and so $\sigma^{n-m}(g_m)$ has an inverse $(\sigma^{n-m}(g_m))^{-1}$ in R. Let $h_1 = f_n(\sigma^{n-m}(g_m))^{-1} x^{n-m}$. Then

$$
\begin{aligned}
& f - h_1 g \\
&= f - f_n(\sigma^{n-m}(g_m))^{-1} x^{n-m}(g_m x^m + g_{m-1}x^{m-1} + \cdots + g_0) \\
&= f - f_n(\sigma^{n-m}(g_m))^{-1}(x^{n-m} g_m x^m + [\text{terms of lower degrees}]) \\
&= f - f_n(\sigma^{n-m}(g_m))^{-1} \left(\sum_{i=0}^{n-m} \binom{n-m}{i} \sigma^i \delta^{n-m-i}(g_m) x^{i+m} + [\text{terms of lower degrees}] \right) \\
&= f - f_n(\sigma^{n-m}(g_m))^{-1}(\sigma^{n-m}(g_m)x^n + \ [\text{terms of lower degrees}]) \\
&= f - f_n x^n - \ [\text{terms of lower degrees}],
\end{aligned}
$$

and so $d(f - h_1 g) < d(f)$. The existence of an element h_2 in S such that $d(f - gh_2) < d(f)$ can be shown analogously.

1.3.2 Ore Domains

Recall that the skew polynomial ring S is a PID (Proposition 1.7). In this section, we shall use this fact.

Let us start with some basic definitions. Let X be a multiplicative set in a ring P (i.e., a subset $X \subseteq P$ such that $1 \in X$ and X is closed under multiplication). Then X is called a *left (right, resp.) Ore set* if for each $a \in X$ and $r \in P$,

$$Xr = Pa \ (rX = aP, \text{ resp.}).$$

If X is a right and left Ore set, then X is called an Ore set.

Definition 1.4. *A left (right, resp.) Ore domain is any domain D in which the non-zero elements form a left (right, resp.) Ore set, i.e., for each nonzero $a, b \in D$, $Da \bigcap Db \neq 0$ ($aD \bigcap bD \neq 0$, resp.). A left and right Ore domain is called an Ore domain.*

Recall that a *left (right, resp.) Bézout domain* is a domain in which every finitely generated left (right, resp.) ideal of R is principal. Since the skew polynomial ring S is a PID, it is a Bézout domain. Every Bézout domain is Ore ([14], Exercise 6D). Thus, we have the following result.

Proposition 1.9. *The skew polynomial ring S is an Ore domain.*

1.3.3 Rings of Fractions

The fact that the skew polynomial ring S is an Ore domain enables us to construct a ring of fractions for S and investigate problems over S from the perspective of a division ring. In this section, we shall outline some properties of rings of fractions and give some results on a ring of fractions for the ring S.

We first fix the following notation for this section:

P	a ring
$X(\subseteq P)$	a multiplicative set of non-zero divisors in P

A *left (right, resp.) ring of fractions* (or *a left (right, resp.) quotient ring*) for P with respect to X is any overring $P' \supseteq P$ such that:

(a) Every element x in X has an inverse x^{-1} in P'.

(b) Every element of P' can be expressed in the form $x^{-1}a$ (resp., ax^{-1}) for some $a \in P$ and $x \in X$.

Proposition 1.10. *([14], Theorem 6.2) A left (right, resp.) ring of fractions for P with respect to X exists if and only if X is a left (right, resp.) Ore set.*

If $X(\subseteq P)$ is a left (right, resp.) Ore set, we shall write $X^{-1}P$ (PX^{-1}, resp.) to denote any left (right, resp.) ring of fractions for P with respect to X.

Proposition 1.11. *([14], Proposition 6.5) If $X(\subseteq P)$ is a right and left Ore set, then $PX^{-1} = X^{-1}P$, and vice versa.*

We now turn to classical quotient rings. A *classical left (right, resp.) quotient ring* for P is a left (right, resp.) quotient ring for P with respect to the multiplicative set of all non-zero divisors in P. If P has both a classical left quotient

ring and a classical right quotient ring, then by Proposition 1.11, the two one-sided classical quotient rings coincide; In this case, P is said to have a *classical quotient ring.*

Proposition 1.12. *([14], Theorem 6.8) For a ring P, the following conditions are equivalent:*

(a) There exists a right (left, resp.) Ore set X of non-zero divisors in P such that PX^{-1} ($X^{-1}P$, resp.) is a division ring.

(b) P has a classical right (left, resp.) quotient ring which is a division ring.

(c) P is a right (left, resp.) Ore domain.

Recall that the skew polynomial ring S is a left and right Ore domain (Proposition 1.9). By Proposition 1.10, there exist a classical left (right, resp.) quotient ring for S with respect to $S \setminus \{0\}$; Moreover, by Proposition 1.11, the classical left (right, resp.) quotient ring is also a right (left, resp.) quotient ring. Thus, we just refer to *the Ore quotient ring* of S, and use $Q(S)$ to denote it for the rest of this paper.

1.4 Inverse of a Matrix

The inverse for a matrix is sometimes needed in the investigation of a generalized inverse for a matrix. In this section, we give some properties of the inverse of a matrix over the skew polynomial ring S, together with some relevant definitions.

Let A be an $n \times n$ matrix over a ring P. A *left (right, resp.) inverse* of A over P is an $n \times n$ matrix A_L^{-1} (A_R^{-1}, resp.) such that $A_L^{-1}A = I$ ($AA_R^{-1} = I$, resp.). An *inverse* of A over P is an $n \times n$ matrix A^{-1} over P such that $A^{-1}A = AA^{-1} = I$. If both A_L^{-1} and A_R^{-1} exist, then $A_L^{-1} = A_R^{-1} = A^{-1}$, and A is called an *invertible* matrix over P. The uniqueness of an inverse for a matrix is obvious.

For any matrix A over the skew polynomial ring S, a left (or right) inverse of A is in fact the inverse of A over S. To prove this, we use the fact that S is

Noetherian and thus is stably finite.

Definition 1.5. *A ring P is said to be right Noetherian if it satisfies the ascending chain condition (ACC) on right ideals, namely, whenever $I_1 \subset I_2 \subset \cdots$ is a strictly increasing chain of right ideals of P, there exists a positive integer m such that $I_n = I_m$ for all $n \geq m$. A left Noetherian ring is defined correspondingly.*

Using the property that S is a PID, we can verify the following conclusion without difficulty.

Proposition 1.13. *The skew polynomial ring S is left and right Noetherian.*

We now give the property that S is stably finite.

Definition 1.6. *([20], p. 5) A ring P is Dedekind-finite if, for any $a, b \in P$, $ab = 1$ implies $ba = 1$. We say that a ring Q is stably finite if the matrix rings $\mathbb{M}_n(Q)$ are Dedekind-finite for all natural numbers n.*

Proposition 1.14. *([20], Proposition 1.13) The skew polynomial ring S is stably finite, that is, for any $n \times n$ matrix A over the skew polynomial ring S, a left (or right) inverse of A over S is the inverse of A over S.*

For matrices over S, there are three types of *elementary row (column, resp.) operations* defined as follows:

(i) Interchange of any two rows (columns, resp.)

(ii) Addition of a multiple of a row (column, resp.) by a non-zero polynomial from S to another row (column, resp.)

(iii) Scalar multiplication from the left (right, resp.) of a row (column, resp.) by a non-zero element from R.

An *elementary matrix* over S is a square matrix obtained by applying one single elementary row (or column) operation on an identity matrix. A matrix

over S is called a *unimodular matrix* if it is a product of elementary matrices over S.

It is known that every elementary (unimodular, resp.) matrix over a field $\mathbb{F}$ has an inverse that is also elementary (unimodular, resp.) over $\mathbb{F}$. A proof of this result can be found in any elementary linear algebra book. For matrices over S, we have a similar result (which can be shown analogously) as follows.

Proposition 1.15. *(a) Every elementary matrix over S is invertible over S. Moreover, the inverse of an elementary matrix over S is also an elementary matrix over S.*

(b) Every unimodular matrix over S is invetible over S. Moreover, the inverse of a unimodular matrix over S is also a unimodular matrix over S.

The above proposition can be shown in a similar way as we did for the commutative case (which can be found in any standard elementary linear algebra book).

1.5 Rank of a Matrix

In this section, we give the result that the skew polynomial ring S is a free ideal ring. By interpreting matrices over S as S-module homomorphisms, we define three types of rank of a matrix over S and show that the ranks are in fact equivalent.

1.5.1 Free Ideal Rings

Let P be a ring. An indexed set $X = (x_i)_{i\in I}$ of elements of a module over P is called *left (right, resp.) linearly independent* if for every finite sequence $x_1, ..., x_n$ of elements of X and every $p_1, ..., p_n \in P$,

$$\sum_{i=1}^{n} p_i x_i = 0 \ (\sum_{i=1}^{n} x_i p_i = 0, \text{ resp.}) \text{ implies } p_1 = \cdots = p_n = 0.$$

A *free left P-module (of rank cardinality I)* is a left P-module M with a linearly independent spanning set $X = (x_i)_{i\in I}$. In other words, M is a free left P-module if M is isomorphic to $\oplus_{i\in I} Px_i$. If I is finite, that is, $M \cong \oplus_{i=1}^{n} Px_i$ for some $n \in \mathbb{N}$, then n is called the *rank* of M, written $n = \text{rank}(M)$. A *free right P-module N* and the rank of N are defined correspondingly.

Definition 1.7. *([10], P. 110) A free left ideal ring (a left fir, for short) is a ring P in which all left ideals are free as left P-modules, of unique rank. A right fir is defined correspondingly. A free ideal ring (a fir, for short) is a left and right fir.*

Since S is a left and right Ore domain, we have the following result.

Proposition 1.16. *([10], Proposition 2.2.2.) The skew polynomial ring S is a fir.*

Definition 1.8. *([10], P. 111) Let α be a cardinal. A left α-fir is a ring P in which all α-generated left ideals are free as left P-modules, of unique rank. A right α-fir is defined correspondingly. An α-fir is a left and right α-fir.*

Clearly, S is an α-fir.

Proposition 1.17. *([8], Theorem 2.1) Let α be a cardinal.*

(i) In a left fir every submodule of a free left module is free.

(ii) In a left α-fir every α-generated submodule of a free left module is free.

1.5.2 Rank of a Matrix

After seeing that the skew polynomial ring S is a free ideal ring, we can define the rank of a matrix over S. We fix the following notation for this section.

S^m	the set of $1 \times m$ matrices over S
${}^nS$	the set of $n \times 1$ matrices over S
$\underline{0}$	a zero matrix of suitable size

Both ${}^nS$ and S^m are free S-modules, thus, any n-generated submodule of ${}^nS$ and any m-generated submodule of S^m are free (Proposition 1.17).

We interpret a matrix $A_{m\times n}$ over S in the following ways:

(a) a right S-module homomorphism of columns ${}^nS \to {}^mS$, that is, a function $f : {}^nS \to {}^mS$ such that $f(u+v) = f(u) + f(v)$ and $f(va) = f(v)a$ for all $u, v \in {}^nS$ and $a \in S$,

(b) a left S-module homomorphism of rows $S^m \to S^n$.

(c) an element of the $(\mathbb{M}_m(S), \mathbb{M}_n(S))$-bimodule ${}^mS \otimes S^n$.

The *column rank* of A over S is the rank of the submodule of ${}^mS$ spanned by the n columns of A, that is, the rank of the image of A under the above interpretation (a). The *row rank* of A over S is the rank of the submodule of S^n generated by the m rows of A under the above interpretation (b). Since S is an n-fir for any $n \in \mathbb{N},\ n \geq 1$, the definitions of column rank and row rank of a matrix over S are valid. Note that the column (row, resp.) rank of the matrix is independent of the choice of bases. In particular, the column (row, resp.) rank is not affected by elementary operations.

We now define the inner rank of a matrix. Let $A = B_{m\times r}C_{r\times n}$ be a decomposition of A over S, where r is the least number that such a matrix C can have. The number r is called the *inner rank* of A, written $r = \rho(A)$, and the factorization BC is called the *rank factorization* of A over S.

Proposition 1.18. *([10], Proposition 5.4.3.) Let $A \in \mathbb{M}_{m\times n}(S)$. The following four numbers are equal and do not exceed* $\min\{\rho_r(A), \rho_c(A)\}$*, where $\rho_r(A)$ denotes the row rank of A and $\rho_c(A)$ denotes the column rank of A:*

(i) the least r such that the map A (under interpretation (a) or (b)) can be factored through S^r,

(ii) the least r such that A can be written $\sum_{i=1}^{r} b_i \otimes c_i$, under interpretation (c),

(iii) the least r such that the image of A in S^n is contained in a submodule generated by r elements (interpretation (b)),

(iv) the least r such that the image of A in ${}^mS$ is contained in a submodule generated by r elements (interpretation (a)).

In Part (ii) of Proposition 1.18, the number r is equivalent to the least number r such that $A = B_{m\times r}C_{r\times n}$ and thus is in fact the inner rank of A. Therefore, for any $m \times n$ matrix A,

$$0 \leq \rho(A) \leq \min\{m, n\}, \tag{1.15}$$

and

$$\rho(A) = 0 \text{ if and only if } A = \underline{0}. \tag{1.16}$$

Also, using rank factorization, we can verify that for any two matrices A and B,

$$\rho(\text{diag}(A, B)) \leq \rho(A) + \rho(B), \tag{1.17}$$

$$\rho(AB) \leq \min\{\rho(A), \rho(B)\}. \tag{1.18}$$

We now turn to the relation between the three types of rank defined above. Since the skew polynomial ring S is a Bézout domain, we have the following result.

Proposition 1.19. *([10], Proposition 5.4.4) Over the skew polynomial ring S, the row rank, the column rank and the inner rank of a matrix are equal.*

From above we can see that, for any matrix A over S,

$$\rho(A) = \rho(A^T). \tag{1.19}$$

Also, since the three types of rank of A coincide, we shall just refer to the *rank* of A and use $\rho(A)$ to denote it in the rest of the thesis.

Definition 1.9. *Let $A \in \mathbb{M}_{m\times n}(S)$, where $m, n \in \mathbb{N}$, $1 \leq m \leq n$ ($1 \leq n \leq m$). Then A is said to be of left (right. resp.) full rank if $\rho(A) = m$ ($\rho(A) = n$). If $m = n$ and $\rho(A) = n$, then A is of full rank.*

Lemma 1.5. *([10], Corollary 5.4.5) Let $A_{m\times n}$, $B_{k\times m}$ and $C_{k\times m}$ ($k, m, n \in \mathbb{N}$) be matrices over S. Then $BA = CA$ ($AB = AC$, resp.) implies $B = C$ if and only if A is of left (right, resp.) full rank.*

Chapter 2

An Algorithm For Finding $\{1\}$-inverses (Commutative Case)

An algorithm for finding a $\{1\}$-inverse of a matrix over a (commutative) ring has been introduced by K. P. S. B. Rao ([30], p. 41). In this chapter, we shall improve the efficiency of the algorithm given by K. P. S. B. Rao and use it to find $\{1\}$-inverses of matrices over a polynomial ring $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. In fact, all of the results of this chapter hold for matrices over any commutative Euclidean domain. The Maple code of the improved algorithm will be given in Appendix.

2.1 Theoretical Basis

Let us start with some properties of matrices over the polynomial ring $\mathbb{F}[x]$.

Lemma 2.1. *Let $A_{m\times n}, B_{m\times n}$ $(m, n \in \mathbb{N})$ be two matrices over $\mathbb{F}[x]$ such that $B = E_{m\times m}AF_{n\times n}$, where*

(i) E is a square matrix over $\mathbb{F}[x]$ obtained by applying row exchanging and/or row addition to an identity matrix,

(ii) F is a square matrix over $\mathbb{F}[x]$ obtained by applying column exchanging and/or column addition to an identity matrix.

Then

(a) E and F are invertible in $\mathbb{M}_{m\times m}(\mathbb{F}[x])$ and $\mathbb{M}_{n\times n}(\mathbb{F}[x])$, respectively;

(b) A has a $\{1\}$-inverse over $\mathbb{F}[x]$ if and only if B has a $\{1\}$-inverse over $\mathbb{F}[x]$.

Proof. We first show that E is invertible over $\mathbb{F}[x]$. By definition, E is a product of elementary matrices whose determinants are 1. Thus, $\det(E) = \pm 1$, and so E is invertible over $\mathbb{F}[x]$ with $E^{-1} = \frac{1}{\det(E)}\operatorname{adj}(E) = \pm\operatorname{adj}(E)$, where $\operatorname{adj}(E)$ denotes the adjoint matrix of E. Similarly, we can show that F is invertible over $\mathbb{F}[x]$.

If B has a $\{1\}$-inverse G_B over $\mathbb{F}[x]$, then $(EAF)G_B(EAF) = EAF$, which implies $A(FG_BE)A = A$, that is, A has a $\{1\}$-inverse FG_BE over $\mathbb{F}[x]$.

Conversely, suppose A has a $\{1\}$-inverse G_A over $\mathbb{F}[x]$, namely, $AG_AA = A$. Since $B = EAF$, we have $A = E^{-1}BF^{-1}$. Then $AG_AA = A$ implies $B(F^{-1}G_AE^{-1})B = B$, and so B has a $\{1\}$-inverse $(F^{-1}G_AE^{-1})$ over $\mathbb{F}[x]$. □

Theorem 2.1. *(a) Let $A = \begin{bmatrix} a_1 \cdots a_n \end{bmatrix}$ ($A = \begin{bmatrix} a_1 \cdots a_n \end{bmatrix}^T$, resp.) be a $1 \times n$ ($n \times 1$, resp.) matrix over $\mathbb{F}[x]$ with $a_1 \neq 0$. If A has a $\{1\}$-inverse over $\mathbb{F}[x]$, then $\gcd(a_1, ..., a_n) = 1$.*

(b) Let $A = \begin{bmatrix} a & \underline{z} \\ 0_{m\times 1} & B_{m\times n} \end{bmatrix}$ be a matrix over $\mathbb{F}[x]$ with $a \neq 0$ and $\underline{z} = \begin{bmatrix} z_1 \cdots z_n \end{bmatrix}$. If A has a $\{1\}$-inverse over $\mathbb{F}[x]$, then $\gcd(a, z_1, ..., z_n) = 1$.

(c) Let $\begin{bmatrix} a & 0_{1\times n} \\ 0_{m\times 1} & B_{m\times n} \end{bmatrix}$ be a matrix over $\mathbb{F}[x]$. If A has a $\{1\}$-inverse, then (i) either $a = 0$ or a has a multiplicative inverse in $\mathbb{F}[x]$ and (ii) B has a $\{1\}$-inverse over $\mathbb{F}[x]$.

Proof. (a) We shall only show the case for $A = \begin{bmatrix} a_1 \cdots a_n \end{bmatrix}$. The case for $A = \begin{bmatrix} a_1 \cdots a_n \end{bmatrix}^T$ can be shown analogously.

Let $G = \begin{bmatrix} g_1 \cdots g_n \end{bmatrix}^T$ be a $\{1\}$-inverse of A. Then

$$\begin{bmatrix} a_1 \cdots a_n \end{bmatrix} = \begin{bmatrix} a_1 \cdots a_n \end{bmatrix} \begin{bmatrix} g_1 \cdots g_n \end{bmatrix}^T \begin{bmatrix} a_1 \cdots a_n \end{bmatrix} = \begin{bmatrix} (a_1g_1 + \cdots + a_ng_n)a_1 \cdots \end{bmatrix}.$$

It follows that $a_1 = (a_1g_1 + \cdots + a_ng_n)a_1$, that is, $(a_1g_1 + \cdots + a_ng_n - 1)a_1 = 0$. Since $\mathbb{F}[x]$ has no zero divisors, and since $a_1 \neq 0$, we have $a_1g_1 + \cdots + a_ng_n = 1$. Since $\mathbb{F}[x]$ is a principal ideal domain, $\gcd(a_1, ..., a_n) = 1$ ([30], Theorem 4.2).

(b) By [30], Theorem 4.15.

(c) By [30], Theorem 4.15.

□

Theorem 2.2. *Let $A_{m\times n} = (a_{ij})$ be a matrix over $\mathbb{F}[x]$.*

(a) There exists an invertible matrix $E_{m\times m}$ over $\mathbb{F}[x]$, such that

$$EA = \begin{bmatrix} g & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{bmatrix}$$

where $g = \gcd(a_{11}, a_{21}, ..., a_{m1})$ and each $*$ stands for some element in $\mathbb{F}[x]$.

(b) There exists an invertible matrix $F_{n\times n}$ over $\mathbb{F}[x]$, such that

$$AF = \begin{bmatrix} h & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{bmatrix}$$

where $h = \gcd(a_{11}, a_{12}, ..., a_{1n})$ and each $*$ stands for some element in $\mathbb{F}[x]$.

Proof. (a) Since $\mathbb{F}[x]$ is a Euclidean domain, by the traditional extended Euclidean algorithm for commutative Euclidean domains (for example, [31], Algorithm 3.6), we can find some $g_1, s_1, t_1 \in \mathbb{F}[x]$ such that

$$\gcd(a_{11}, a_{21}) = g_1 = s_1a_{11} + t_1a_{21}.$$

Define E_1 to be an $m \times m$ elementary matrix over $\mathbb{F}[x]$ such that

$$E_1(i,j) = \begin{cases} s_1, & i = 1,\ j = 1, \\ t_1, & i = 1,\ j = 2, \\ -\frac{a_{21}}{g_1}, & i = 2,\ j = 1, \\ \frac{a_{11}}{g_1}, & i = 2,\ j = 2, \\ 1, & 3 \le i \le m,\ j = i, \\ 0, & \text{otherwise.} \end{cases} \text{, i.e., } E_1 = \begin{bmatrix} s_1 & t_1 & 0 & \cdots & 0 \\ -\frac{a_{21}}{g_1} & \frac{a_{11}}{g_1} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then

$$E_1 A = \begin{bmatrix} s_1 & t_1 & 0 & \cdots & 0 \\ -\frac{a_{21}}{g_1} & \frac{a_{11}}{g_1} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

$$= \begin{bmatrix} g_1 & * & \cdots & * \\ 0 & * & \cdots & * \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},$$

where each $*$ stands for some element in $\mathbb{F}[x]$.

Using the same idea, we define $m \times m$ elementary matrices E_k over $\mathbb{F}[x]$ for $k = 1, ..., m-1$ as follows

$$E_k(i,j) = \begin{cases} s_k, & i = 1,\ j = 1, \\ t_k, & i = 1,\ j = k, \\ -\frac{a_{k+1,1}}{g_k}, & i = k,\ j = 1, \\ \frac{g_{k-1}}{g_k}, & i = k,\ j = k, \\ 1, & 2 \le i \le m,\ i \ne k,\ j = i, \\ 0, & \text{otherwise}, \end{cases}$$

where $s_k, t_k, g_k \in \mathbb{F}[x]$ such that

$$g_k = \gcd(g_{k-1}, a_{k+1,1}) = s_k g_{k-1} + t_k a_{k+1,1}.$$

Then for each k,

$$E_k \cdots E_1 A = \begin{bmatrix} g_k & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \\ a_{k+2,1} & a_{k+2,2} & \cdots & a_{k+2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

where $g_k = \gcd(a_{11}, a_{21}, ..., a_{k+1,1})$. Let $E = E_{m-1} \cdots E_1$. Then E is the desired unimodular matrix.

(b) Similarly, we can show the existence of the matrix F. Since $\mathbb{F}[x]$ is a Euclidean domain, by the traditional extended Euclidean algorithm for commutative Euclidean domains, we can find some $h_1, p_1, q_1 \in \mathbb{F}[x]$ such that

$$\gcd(a_{11}, a_{12}) = h_1 = p_1 a_{11} + q_1 a_{12}.$$

Define F_1 to be an $n \times n$ elementary matrix over $\mathbb{F}[x]$ such that

$$F_1(i,j) = \begin{cases} p_1, & i = 1,\ j = 1, \\ q_1, & i = 2,\ j = 1, \\ -\frac{a_{12}}{h_1}, & i = 1,\ j = 2, \\ \frac{a_{11}}{h_1}, & i = 2,\ j = 2, \\ 1, & 3 \le i \le m,\ j = i, \\ 0, & \text{otherwise.} \end{cases} \text{, i.e., } F_1 = \begin{bmatrix} p_1 & -\frac{a_{12}}{h_1} & 0 & \cdots & 0 \\ q_1 & \frac{a_{11}}{h_1} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Then

$$AF_1 = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} p_1 & -\frac{a_{12}}{h_1} & 0 & \cdots & 0 \\ q_1 & \frac{a_{11}}{h_1} & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$= \begin{bmatrix} h_1 & 0 & a_{13} & \cdots & a_{1n} \\ * & * & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & a_{m3} & \cdots & a_{mn} \end{bmatrix},$$

where each $*$ stands for some element in $\mathbb{F}[x]$.

Using the same idea, we define $n \times n$ elementary matrices F_k over $\mathbb{F}[x]$ for $k = 2, ..., n-1$ as follows

$$F_k(i,j) = \begin{cases} p_k, & i = 1,\ j = 1, \\ q_k, & i = k,\ j = 1, \\ -\frac{a_{1,k+1}}{h_k}, & i = 1,\ j = k, \\ \frac{h_{k-1}}{h_k}, & i = k,\ j = k, \\ 1, & 2 \le i \le n,\ i \ne k,\ j = i, \\ 0, & \text{otherwise}, \end{cases}$$

where $p_k, q_k, h_k \in \mathbb{F}[x]$ such that

$$h_k = \gcd(h_{k-1}, a_{1,k+1}) = p_k h_{k-1} + q_k a_{1,k+1}.$$

Let $F = F_1 \cdots F_{n-1}$. Then F is the desired unimodular matrix.

□

2.2 Algorithm

We now give the algorithm for finding a $\{1\}$-inverse of a matrix over the polynomial ring $\mathbb{F}[x]$.

Algorithm 1 Row operations (RowOp)

Input $A \in \mathbb{M}_{m\times n}(\mathbb{F}[x])$ and $k, i \in \mathbb{N}$, where $m, n \in \mathbb{N},\ m \ge 2, n \ge 1,\ 1 \le k \le m-1,\ k+1 \le i \le m$, and at least one of $A(k,k), A(i,k)$ is nonzero.

Output A unimodular matrix $Ro \in \mathbb{M}_{m\times m}(\mathbb{F}[x])$ such that

$$(RoA)(k,k) = \gcd(A(k,k), A(i,k)) \text{ and } (RoA)(i,k) = 0.$$

1: Use the extended Euclidean algorithm to compute g, s, t such that

$$g = \gcd(A(k,k), A(i,k)) = sA(k,k) + tA(i,k).$$

2: $Ro \leftarrow I_m$
3: $Ro(k,k) \leftarrow s,\ Ro(k,i) \leftarrow t,\ Ro(i,k) \leftarrow -\frac{A(i,k)}{g},\ Ro(i,i) \leftarrow \frac{A(k,k)}{g}$
4: **return** Ro

Algorithm 2 Column operations (ColOp)

Input $A \in \mathbb{M}_{m\times n}(\mathbb{F}[x])$ and $k, j \in \mathbb{N}$, where $m, n \in \mathbb{N},\ m \geq 1, n \geq 2,\ 1 \leq k \leq n-1,\ k+1 \leq j \leq n$, and at least one of $A(k,k), A(k,j)$ is nonzero.

Output A unimodular matrix $Co \in \mathbb{M}_{n\times n}(\mathbb{F}[x])$ such that

$$(ACo)(k,k) = \gcd(A(k,k), A(k,j)) \text{ and } (ACo)(k,j) = 0.$$

1: Use the extended Euclidean algorithm to compute g, s, t such that

$$g = \gcd(A(k,k), A(k,j)) = sA(k,k) + tA(k,j).$$

2: $Co \leftarrow I_n$
3: $Co(k,k) \leftarrow s$, $Co(k,j) \leftarrow -\frac{A(k,j)}{g}$, $Co(j,k) \leftarrow t$, $Co(j,j) \leftarrow \frac{A(k,k)}{g}$
4: **return** Co

Algorithm 3 Find a $\{1\}$-inverse of a given matrix

Input $A \in \mathbb{M}_{m\times n}(\mathbb{F}[x])$ and $m, n \in \mathbb{N}$.

Output $\begin{cases} G \in \mathbb{M}_{n\times m}(\mathbb{F}[x]) \text{ such that } AGA = A, \text{ if } A \text{ has a } \{1\}\text{-inverse;} \\ \text{“The given matrix has no } \{1\}\text{-inverse. ”, otherwise.} \end{cases}$

Steps

1: $s \leftarrow \min\{m, n\}$
2: $Ro \leftarrow I_m$, $Co \leftarrow I_n$, $E \leftarrow I_m$, $F \leftarrow I_n$
3: **if** $A = \begin{bmatrix} \end{bmatrix}$ **or** $A = 0_{m\times n}$ **then** ▷ A: an empty matrix or a zero matrix.
4: **return** $G \leftarrow A^T$
5: **end if**

6: $B \leftarrow A$
7: **if** $s > 1$ **then**
8: **for** k **from** 1 **to** $s-1$ **do**

9: **if** $\mathrm{Col}_k(B) = \underline{0}$ and $\mathrm{Row}_k(B) = \underline{0}^T$ **then**
10: $k \leftarrow k+1$ and goto step 7
11: **end if**

12: **for** i **from** $k+1$ **to** m **do**
13: **Call** Algorithm 1 to compute $Ro \leftarrow \mathrm{RowOp}(B, k, i)$
14: $B \leftarrow RoB$
15: $E \leftarrow RoE$
16: **end for**

17: $C \leftarrow B$
18: **for** j **from** $k+1$ **to** n **do**
19: **Call** Algorithm 2 to compute $Co \leftarrow \mathrm{ColOp}(C, k, j)$
20: $C \leftarrow CCo$
21: $F \leftarrow FCo$
22: **end for**

Algorithm 3 Find a $\{1\}$-inverse of a given matrix (continued)

if $C(k,k) \neq 1$ **then**
  return "The input matrix has no $\{1\}$-inverse." ▷ Theorem 2.1.
else
  for i **from** $k+1$ **to** m **do**
    Call Algorithm 1 to compute $Ro \leftarrow \mathrm{RowOp}(C,k,i)$
    $C \leftarrow RoC$
    $E \leftarrow RoE$
  end for
  $B \leftarrow C$
end if
end for
end if
if $m = n$ **then** ▷ $m = n = s$.
if $B(s,s) \in \mathbb{F}$ **then**
if $B(s,s) \neq 0$ **then**
  $Ro \leftarrow$ the matrix obtained by multiplying $\mathrm{Row}_s(I_m)$ by $\frac{1}{B(s,s)}$
  $B \leftarrow RoB,\ E \leftarrow RoE$
end if
return $G \leftarrow FB^TE$
else ▷ $B(s,s) \notin \mathbb{F}$.
return "The input matrix has no $\{1\}$-inverse." ▷ Theorem 2.1.
end if
else
if $m > n$ **then**
  $B \leftarrow B^T$
end if
$rB \leftarrow$ row dimension of B, $cB \leftarrow$ column dimension of B ▷ $rB < cB$.
if $\mathrm{Row}_{rB}(B) = \underline{0}$ **then**
if $m > n$ **then**
  return $G \leftarrow FBE$
else
  return $G \leftarrow FB^TE$
end if
else
for j **from** $rB+1$ **to** cB **do**
  Call Algorithm 2 to compute $Co \leftarrow \mathrm{ColOp}(B,rB,j)$
  $B \leftarrow BCo$
  if $m > n$ **then**
    $E \leftarrow Co^TE$
  else
    $F \leftarrow FCo$
  end if
end for

Algorithm 3 Find a {1}-inverse of a given matrix (continued)

66: **if** $B(rB, rB) \neq 1$ **then**
67: **return** "The input matrix has no {1}-inverse."
68: **else if** $m > n$ **then**
69: **return** $G \leftarrow FBE$
70: **else**
71: **return** $G \leftarrow FB^TE$
72: **end if**
73: **end if**

74: **end if**

Theorem 2.3. *In Algorithm 3, if the given matrix A has a $\{1\}$-inverse over $\mathbb{F}[x]$, then the matrix G is a $\{1\}$-inverse of A over $\mathbb{F}[x]$.*

Proof. From Algorithm 3 we can see that, the matrices $E_{m\times m}$, $F_{n\times n}$ and $B_{m\times n}$ obtained at Step 4 / 41 / 52 / 54 / 69 / 71 satisfy the following conditions:

(a) E and F are invertible over $\mathbb{F}[x]$,

(b) $EAF = B$,

(c) $B(i,j) = \begin{cases} 1 \text{ or } 0, \text{ for } i = 1, ..., s \text{ and } j = i \ (s = \min\{m, n\}) \\ 0, \text{ otherwise} \end{cases}$.

If $m \leq n$, then $s = m$ and so $BB^T = I_m$, which implies $BB^TB = I_m$; otherwise, $m > n = s$, and so $B^TB = I_n$, which also gives $BB^TB = B$. Thus, B^T is a $\{1\}$-inverse of B, i.e., $BB^TB = B$. Then, from $EAF = B$ we can get

$$(EAF)B^T(EAF) = EAF.$$

By Theorem 2.1, E and F have inverses E^{-1} and F^{-1} over $\mathbb{F}[x]$, respectively. So $E^{-1}(EAF)\ B^T\ (EAF)F^{-1} = E^{-1}EAFF^{-1}$, that is,

$$A(FB^TE)A = A.$$

Hence, $G = FB^TE$ is a $\{1\}$-inverse of A. □

2.3 Examples

Below are some examples generated by using the algorithm.

(a) Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ be a matrix over $\mathbb{Q}$.

Then $G_A = \begin{bmatrix} -1 & \frac{1}{2} \\ 0 & 0 \\ \frac{2}{3} & -\frac{1}{6} \end{bmatrix}$ is a $\{1\}$-inverse of A over $\mathbb{Q}$.

(b) Let $B = \begin{bmatrix} 1 & x \\ 0 & 1 \\ 5 & 6 \end{bmatrix}$ be a matrix over $\mathbb{Q}[x]$.

Then $G_B = \begin{bmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \end{bmatrix}$ is a $\{1\}$-inverse of B over $\mathbb{Q}[x]$.

(c) Let $C = \begin{bmatrix} 3x^5 - 6x^4 + 4x^3 + 6x^2 + 1 & -x^4 + 2x^3 - x^2 - 2x & x^3 - 2x^2 + 2 & x^2 + 1 \\ -3x^3 + 3x^2 - 4x & x^2 - x + 1 & -x + 1 & x \\ 3x^2 & -x & 1 & x^3 \end{bmatrix}$ be a matrix over $\mathbb{Q}[x]$. Then $G_C = \begin{bmatrix} 1 & x^2 & x^2 - 2 \\ 4x & 4x^3 + 1 & 4x^3 - 7x - 1 \\ x^2 & x^4 + x & x^4 - x^2 - x + 1 \\ 0 & 0 & 0 \end{bmatrix}$ is a $\{1\}$-inverse of C over $\mathbb{Q}[x]$.

(d) Let $D = \begin{bmatrix} 1 & x \\ x & 1 \end{bmatrix}$ be a matrix over $\mathbb{Q}[x]$. By Algorithm 3,

$$\begin{bmatrix} 1 & x \\ x & 1 \end{bmatrix} \xrightarrow{\text{Row}_2 - x\,\text{Row}_1 \to \text{Row}_2} \begin{bmatrix} 1 & x \\ 0 & -x^2 + 1 \end{bmatrix} \xrightarrow{\text{Col}_2 - x\,\text{Col}_1 \to \text{Col}_2} \begin{bmatrix} 1 & 0 \\ 0 & -x^2 + 1 \end{bmatrix}.$$

Since $\deg(-x^2+1) > 0$, $\begin{bmatrix} -x^2 + 1 \end{bmatrix}$ has no $\{1\}$-inverse over $\mathbb{Q}[x]$. By Theorem 2.1, D has no $\{1\}$-inverse over $\mathbb{Q}[x]$.

Chapter 3

An Algorithm For Finding {1}-inverses (Non-commutative Case)

Recall that $S = R[x; \sigma, \delta]$ denotes the skew polynomial ring where R is a skew field, σ is an automorphism of R and δ is a σ-derivation. In this chapter, we construct an algorithm for finding $\{1\}$-inverses for matrices over the skew polynomial ring S based on the fact that S is a Euclidean domain (Proposition 1.8).

3.1 Theoretical Basis

In this section, we shall discuss some properties of generalized inverses, which will be used to formulate an algorithm for finding a $\{1\}$-inverse of a given matrix over the skew polynomial ring S.

3.1.1 GCRD, GCLD, LCRM and LCLM

Let $f, g \in S$. A *greatest common right divisor* (GCRD) of $f,\ g$, written $\mathrm{gcrd}(f, g)$, is the normal form $\mathrm{nf}(s)$ of a nonzero skew polynomial $s \in S$ such that

(a) s is a common right divisor of f and g, namely, $f = f_1 s$ and $g = g_1 s$ for some

$f_1, g_1 \in S$,

(b) if $t \in S$ is a common right divisor of f and g, then t is a right divisor of s.

In particular, $\mathrm{gcrd}(0, f) = f$. The *greatest common left divisor* (GCLD) of f and g, written $\mathrm{gcld}(f, g)$, is defined correspondingly.

Lemma 3.1. *(Bézout's identity) Let $a_1, a_2, ..., a_n, a \in S$. The following statements are equivalent.*

(i) $Sa_1 + Sa_2 + \cdots + Sa_n = Sa$ *($a_1S + a_2S + \cdots + a_nS = aS$, resp.).*

(ii) $\mathrm{nf}(a) = \mathrm{gcrd}(a_1, a_2, ..., a_n)$ *($\mathrm{nf}(a) = \mathrm{gcld}(a_1, a_2, ..., a_n)$, resp.).*

Moreover, $\mathrm{gcrd}(a_1, a_2, ..., a_n)$ *($\mathrm{gcld}(a_1, a_2, ..., a_n)$, resp.) is unique.*

Proof. We shall only prove the case of GCRD. The case of GCLD can be shown analogously.

(i) $\Rightarrow$ (ii). Suppose (i) holds. Then $a = c_1a_1 + c_2a_2 + \cdots + c_na_n$ for some $c_1, c_2, ..., c_n \in S$. Also, for each $i = 1, 2, ..., n$, $Sa_i \subseteq Sa$, namely, $a_i = ca$ for some $c \in S$, that is, a is a right divisor of a_i. Let $b \in S$ such that b is a common right divisor of $a_1, ..., a_n$. Then b is a right divisor of a. By definition, $\mathrm{nf}(a) = \mathrm{gcrd}(a_1, a_2, ..., a_n)$.

(ii) $\Rightarrow$ (i). Suppose (ii) holds. Since S is a left principal ideal domain, for $a_1, .., a_n \in S$, there exists $c \in S$ such that $Sa_1 + \cdots + Sa_n = Sc$. By the result above, $\mathrm{nf}(c) = \mathrm{gcrd}(a_1, a_2, ..., a_n)$. Thus, c and a are right divisors of each other, namely, $c = sa$ and $a = rc$ for some $r, s \in S$. It follows that $a = rsa$, namely, $(rs - 1)a = 0$. Since S is a domain, $rs = 1$. Therefore, $r, s \in R$. Since GCRDs are monic, $r = s = 1$. Thus, $a = c$, and so $Sa_1 + Sa_2 + \cdots + Sa_n = Sa$. The uniqueness of $\mathrm{gcrd}(a_1, a_2, ..., a_n)$ is also shown by proving $c = a$. □

We now turn to one-sided least common multiples of polynomials from the skew polynomial ring S.

Let $f, g \in S \setminus \{0\}$. A *least common right multiple (LCRM)* of f, g, written $\mathrm{lcrm}(f, g)$ is the normal form $\mathrm{nf}(s)$ of a nonzero skew polynomial $s \in S$ such that

(a) s is a common right multiple of f and g, namely, $s = ff_1 = gg_1$ for some $f_1, g_1 \in S$,

(b) $t \in S$ is a common right multiple of f and g, then t is a right multiple of s.

The *least common left multiple* (LCLM) of f and g, written $\mathrm{lclm}(f, g)$, is defined correspondingly.

Proposition 3.1. *Let $a_1, a_2, ..., a_n, a \in S$. Then the following are equivalent.*

(i) $a_1S \bigcap a_2S \bigcap \cdots \bigcap a_nS = aS$ *($Sa_1 \bigcap Sa_2 \bigcap \cdots \bigcap Sa_n = Sa$, resp.).*

(ii) $\mathrm{nf}(a) = \mathrm{lcrm}(a_1, a_2, ..., a_n)$ *($\mathrm{nf}(a) = \mathrm{lclm}(a_1, a_2, ..., a_n)$, resp.).*

Moreover, $\mathrm{lcrm}(a_1, a_2, ..., a_n)$ *and* $\mathrm{lclm}(a_1, a_2, ..., a_n)$ *are unique.*

Proof. We shall only prove the case of LCRM. The case of LCLM can be shown analogously.

(i) $\Rightarrow$ (ii). Suppose (i) holds. Then for each $i = 1, 2, ..., n$, $aS \subseteq a_iS$, that is, $a = a_ic_i$ for some $c_i \in S$, and so a is a right multiple of a_i. Let b be a common right multiple of $a_1, ..., a_n$. Then for all $i = 1, 2, ..., n$, $bS \subseteq a_iS$, and so $bS \subseteq aS$. Thus, $b = ac$ for some $c \in S$, and whence b is a right multiple of a. By definition, $\mathrm{nf}(a) = \mathrm{lcrm}(a_1, a_2, ..., a_n)$.

(ii) $\Rightarrow$ (i). Suppose (ii) holds. Since S is a right PID, for $a_1, a_2, ..., a_n \in S$, there exists $c \in S$, such that $a_1S \bigcap a_2S \bigcap \cdots \bigcap a_nS = cS$. By the previous result, $\mathrm{nf}(c) = \mathrm{lcrm}(a_1, ..., a_n)$. Thus, c and a are right multiples of each other, namely, $a = cr$ and $c = as$ for some nonzero monic polynomial $r, s \in S$. It follows that $a = asr$, that is, $a(1 - sr) = 0$. Since S has no zero divisor, $sr = 1$, which implies $r, s \in R$. Hence $s = r = 1$, and so $a = c$. Also, the uniqueness of $\mathrm{lcrm}(a_1, a_2, ..., a_n)$ is shown by proving $a = c$. □

3.1.2 Extended Euclidean Algorithm

In the previous section, we gave the definitions of one-sided GCD and LCM of elements from the Euclidean domain S. To compute the GCRD and LCLM,

we can use the following algorithm that is analogous to the traditional extended Euclidean algorithm for commutative Euclidean domain ([31], Algorithm 3.6).

Algorithm 4 Extended Euclidean Algorithm (EEA)

Input $f, g \in S$, where $\deg(f) = n$, $\deg(g) = m$, $m \leq n$, $m, n \in \mathbb{N}$.
Output $k \in \mathbb{N}$, $r_i, s_i, t_i \in S$ for $0 \leq i \leq k+1$, and $q_i \in S$ for $1 \leq i \leq k$, as computed below.

1: $r_0 \leftarrow f$, $s_0 \leftarrow 1$, $t_0 \leftarrow 0$, $r_1 \leftarrow g$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$
2: $i \leftarrow 1$
3: **while** $r_i \neq 0$ **do**
$q_i \leftarrow r_{i-1} \operatorname{quo}_{\mathrm{l}} r_i$, $r_{i+1} \leftarrow r_{i-1} - q_i r_i$
$s_{i+1} \leftarrow s_{i-1} - q_i s_i$, $t_{i+1} \leftarrow t_{i-1} - q_i t_i$, $i \leftarrow i+1$,
where $r_{i-1} \operatorname{quo}_{\mathrm{l}} r_i$ is the left quotient of the division of r_{i-1} by r_i (see page 11)
4: **end while**
5: $k \leftarrow i-1$
6: **return** k, r_i, s_i, t_i for $0 \leq i \leq k+1$, and q_i for $1 \geq i \geq k$.

The above algorithm eventually terminates since $\deg(r_1), \deg(r_2), ..., \deg(r_k)$ are strictly decreasing non-negative integers. For all $1 \leq i \leq k$, we have $s_i f + t_i g = r_i$; in particular, $\operatorname{gcrd}(f, g) = \operatorname{nf}(r_k)$, $\operatorname{lclm}(f, g) = \operatorname{nf}(s_l f) = \operatorname{nf}(t_l g)$ (see Lemma 3.3). To show this, we first give the following lemma.

Lemma 3.2. *Let r_i, s_i, t_i for $0 \leq i \leq k+1$ and q_i for $1 \leq i \leq k$ be as in Algorithm 4. Consider the matrices*

$$R_0 = \begin{bmatrix} s_0 & t_0 \\ s_1 & t_1 \end{bmatrix}, \; Q_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \text{ for } 1 \leq i \leq k$$

in $\mathbb{M}_{2\times 2}(S)$, and $R_i = Q_i \cdots Q_1 R_0$ for $0 \leq i \leq k$. Then

(a) $R_i \begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}$,

(b) $R_i = \begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix}$.

Proof. (By induction) The case for $i = 0$ is clear from step 1 of Algorithm 4. Suppose (a) and (b) holds for $i \geq 1$. Then by the induction hypothesis and the

fact that $R_{i+1} = Q_{i+1}R_i$, we have

$$R_{i+1}\begin{bmatrix} f \\ g \end{bmatrix} = Q_{i+1}\begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix} = \begin{bmatrix} r_{i+1} \\ r_i - q_{i+1}r_{i+1} \end{bmatrix} = \begin{bmatrix} r_{i+1} \\ r_{i+2} \end{bmatrix}.$$

Similarly, we have

$$R_{i+1} = Q_{i+1}R_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{bmatrix}\begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix} = \begin{bmatrix} s_{i+1} & t_{i+1} \\ s_{i+2} & t_{i+2} \end{bmatrix}.$$

□

Lemma 3.3. *In Algorithm 4, the following statements hold.*

(a) $s_i f + t_i g = r_i$ *for all* $1 \leq i \leq k+1$.

(b) $\mathrm{gcrd}(f, g) = \mathrm{nf}(r_k)$.

(c) $\mathrm{lclm}(f, g) = \mathrm{nf}(s_{k+1}f) = \mathrm{nf}(t_{k+1}g)$.

Proof. (a) It follows directly from Lemma 3.2.

(b) By (a) and Lemma 3.2, we have

$$\begin{bmatrix} r_k \\ 0 \end{bmatrix} = \begin{bmatrix} r_k \\ r_{k+1} \end{bmatrix} = \begin{bmatrix} s_k f + t_k g \\ s_{k+1}f + t_{k+1}g \end{bmatrix} = R_k \begin{bmatrix} f \\ g \end{bmatrix} = Q_k \cdots Q_1 R_0 \begin{bmatrix} f \\ g \end{bmatrix}$$
$$= Q_k \cdots Q_1 \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} = Q_k \cdots Q_1 \begin{bmatrix} f \\ g \end{bmatrix}.$$

For each $i \in \{1, ..., k\}$, Q_i is invertible over S, with inverse $Q_i^{-1} = \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}$.

Thus,

$$\begin{bmatrix} f \\ g \end{bmatrix} = Q_1^{-1} \cdots Q_k^{-1} \begin{bmatrix} r_k \\ 0 \end{bmatrix},$$

which implies that r_k is a common right divisor of f and g. On the other hand, by (a), $r_k = s_k f + t_k g$. Thus, any common right divisor of f and g is a right divisor of r_k. Hence, $\text{gcrd}(f, g) = \text{nf}(r_k)$.

(c) By (a), $s_{k+1}f + t_{k+1}g = r_{k+1} = 0$. Thus, $v = s_{k+1}f = -t_{k+1}g$ is a left common multiple of f and g. Meanwhile, $\deg(v) = \deg(f) + \deg(g) - \deg(\text{gcrd}(f, g))$ ([13], p. 468). Thus, $v = \text{lclm}(f, g)$.

□

Example 3.1. *(EEA) Suppose $S = \mathbb{C}[x; \sigma]$ with $\sigma(c) = \overline{c}$, where $\overline{c}$ is the complex conjugate of c. Let $f = ix^2 - i$, $g = ix^2 + x$ be two elements of S. Set $r_0 = f$, $r_1 = g$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$. Then, by Algorithm 4,*

$$
\begin{aligned}
&r_0 = r_1 + (-x - i) = q_1 r_1 + r_2, \ \textit{where } q_1 = 1, \ r_2 = -x - i,\\
&r_1 = (-ix) r_2 = q_2 r_2, \ \textit{where } q_2 = -ix,\\
&s_2 = s_0 - q_1 s_1 = 1,\\
&s_3 = s_1 - q_2 s_2 = ix,\\
&t_2 = t_0 - q_1 t_1 = -1,\\
&t_3 = t_1 - q_2 t_2 = 1 - ix.
\end{aligned}
$$

By Lemma 3.3,

$$
\begin{aligned}
\text{gcrd}(f, g) &= \text{nf}(r_2) = x + i = -f + g,\\
\text{lclm}(f, g) &= \text{nf}(s_3 f) = \text{nf}(ix(ix^2 - i))\\
&= \text{nf}(t_3 g) = \text{nf}((1 - ix)(ix^2 + x))\\
&= x^3 - x.
\end{aligned}
$$

An algorithm for finding GCLD and LCRM of elements from the Euclidean domain S can be constructed analogously. To complete the computations for more complicated cases, for instance, $S = R[x; \sigma, \delta]$ where $\sigma \neq 1, \ \delta \neq 0$, the computer

algebra package "Ore_algebra" (and the package "OreTools", if needed) in Maple can be used.

3.1.3 $\{1\}$-inverses of Matrices over S

Theorem 3.1. *(a) Let* $A = \begin{bmatrix} a & \underline{z} \\ \underline{0} & B \end{bmatrix}$ *be a matrix over* S *with* $a \neq 0$, $\underline{z} = \begin{bmatrix} z_1 \cdots z_n \end{bmatrix}$ *and* $B \in \mathbb{M}_{m\times n}(S)$. *If* A *has a* $\{1\}$*-inverse over* S, *then* $\gcld(a, z_1, ..., z_n) = 1$.

(b) Let $A = \begin{bmatrix} a & \underline{0} \\ \underline{0} & B \end{bmatrix}$ *be a matrix over* S, *where* $B \in \mathbb{M}_{m\times n}(S)$ *and each* $\underline{0}$ *denotes a zero matrix of the appropriate size. If* A *has a* $\{1\}$*-inverse over* S, *then* $a \in R$ *and* B *has a* $\{1\}$*-inverse over* S.

Proof. (a) Let $G = \begin{bmatrix} g & \underline{x} \\ \underline{y}^T & H \end{bmatrix}$ be a $\{1\}$-inverse of A, where $\underline{y} = \begin{bmatrix} y_1 \cdots y_n \end{bmatrix}$ and $H \in \mathbb{M}_{n\times m}(S)$. Since $A = AGA$, we have

$$\begin{bmatrix} a & \underline{z} \\ \underline{0} & B \end{bmatrix} = \begin{bmatrix} a & \underline{z} \\ \underline{0} & B \end{bmatrix} \begin{bmatrix} g & \underline{x} \\ \underline{y}^T & H \end{bmatrix} \begin{bmatrix} a & \underline{z} \\ \underline{0} & B \end{bmatrix} = \begin{bmatrix} aga + \underline{z}\underline{y}^T a & * \\ * & * \end{bmatrix},$$

where each $*$ stands for some element in S. Then $aga + \underline{z}\underline{y}^T a = a$, hence $(ag + \underline{z}\underline{y}^T - 1)a = 0$. Since S has no zero divisor, we have $ag + \underline{z}\underline{y}^T - 1 = 0$, i.e., $ag + z_1y_1 + \cdots + z_ny_n = 1$. By Lemma 3.1, $\gcld(a, z_1, ..., z_n) = 1$.

(b) Let $G = \begin{bmatrix} g & \underline{x} \\ \underline{y}^T & H \end{bmatrix}$ be a $\{1\}$-inverse of A, where $\underline{x} = \begin{bmatrix} x_1 \cdots x_m \end{bmatrix}$, and $H \in \mathbb{M}_{n\times m}(S)$. Since $A = AGA$, we have

$$\begin{bmatrix} a & \underline{0} \\ \underline{0}^T & B \end{bmatrix} = \begin{bmatrix} a & \underline{0} \\ \underline{0}^T & B \end{bmatrix} \begin{bmatrix} g & \underline{x} \\ \underline{y}^T & H \end{bmatrix} \begin{bmatrix} a & \underline{0} \\ \underline{0}^T & B \end{bmatrix} = \begin{bmatrix} aga & * \\ * & BHB \end{bmatrix},$$

where each $*$ stands for some element in S. Thus, we have $aga = a$ and

$BHB = B$, so $(ag-1)a = a(ga-1) = 0$ and B is regular over S. Since S has no zero divisor, either $a = 0$ or $ag = ga = 1$. Therefore $a \in R$.

□

Lemma 3.4. *Let* $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathbb{M}_2(S)$, $g_R = \mathrm{gcrd}(a_{11}, a_{21})$ *and* $g_L = \mathrm{gcld}(a_{11}, a_{12})$. *Then there exist invertible matrices* $E, F \in \mathbb{M}_2(S)$, *such that*

$$EA = \begin{bmatrix} g_R & * \\ 0 & * \end{bmatrix}, \qquad AF = \begin{bmatrix} g_L & 0 \\ * & * \end{bmatrix},$$

where each $*$ *stands for some element in* S.

Proof. We first show the existence of the above matrix E. By Lemma 3.1 and Proposition 3.1, there exist $s, t, k, l \in S$, such that

$$sa_{11} + ta_{21} = g_R, \qquad \mathrm{lclm}(a_{11}, a_{21}) = ka_{11} = la_{21}. \tag{3.1}$$

Assume $a_{11} = b_{11}g_R$, $a_{21} = b_{21}g_R$ for some $b_{11}, b_{21} \in S$. Then $(sb_{11} + tb_{21} - 1)g_R = 0$, and $(kb_{11} - lb_{21})g_R = 0$. Since S is a domain, either $g_R = 0$ or

$$sb_{11} + tb_{21} = 1, \qquad kb_{11} - lb_{21} = 0. \tag{3.2}$$

If $g_R = 0$, then $a_{11} = a_{21} = 0$, and we are done with $E = I_2$. Otherwise, we have (3.2). Also, by (3.1), $\mathrm{gcld}(k, l) = 1$. So there exist $p, q \in S$ such that

$$kp - lq = \mathrm{gcld}(p, q) = 1. \tag{3.3}$$

Let

$$E = \begin{bmatrix} s & t \\ k & -l \end{bmatrix}, \qquad E_1 = \begin{bmatrix} b_{11} & p - b_{11}sp - b_{11}tq \\ b_{21} & q - b_{21}sp - b_{21}tq \end{bmatrix}.$$

Then, by (3.1)–(3.3),

$$EA = \begin{bmatrix} s & t \\ k & -l \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} sa_{11} + ta_{11} & * \\ ka_{11} - la_{21} & * \end{bmatrix} = \begin{bmatrix} g_R & * \\ 0 & * \end{bmatrix}$$

and

$$\begin{aligned} EE_1 &= \begin{bmatrix} s & t \\ k & -l \end{bmatrix} \begin{bmatrix} b_{11} & p - b_{11}sp - b_{11}tq \\ b_{21} & q - b_{21}sp - b_{21}tq \end{bmatrix} \\ &= \begin{bmatrix} sb_{11} + tb_{21} & s(p - b_{11}sp - b_{11}tq) + t(q - b_{21}sp - b_{21}tq) \\ kb_{11} - lb_{21} & k(p - b_{11}sp - b_{11}tq) - l(q - b_{21}sp - b_{21}tq) \end{bmatrix} \\ &= \begin{bmatrix} 1 & sp - (sb_{11} + tb_{21})sp - (sb_{11} + tb_{21})tq + tq \\ 0 & kp - lq - (kb_{11} - lb_{21})sp - (kb_{11} - lb_{21})tq \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Thus, E_1 is a right inverse of E over S. By Proposition 1.14, E_1 is the inverse of E over S.

The existence of the above matrix F can be shown analogously. By Lemma 3.1 and Proposition 3.1, there exist $s', t', k', l' \in S$ such that

$$a_{11}s' + a_{12}t' = g_L, \qquad a_{11}k' = a_{12}l' = \operatorname{lcrm}(a_{11}, a_{12}). \tag{3.4}$$

Suppose $a_{11} = g_L c_{11}$ and $a_{12} = g_L c_{12}$ for some $c_{11}, c_{12} \in S$. Then

$$c_{11}s' + c_{12}t' = 1, \qquad c_{11}k' - c_{12}l' = 0. \tag{3.5}$$

By (3.4), $\operatorname{gcrd}(k', l') = 1$. So there exist some $p', q' \in S$ such that

$$p'k' - l'q' = 1. \tag{3.6}$$

Let

$$F = \begin{bmatrix} s' & k' \\ t' & -l' \end{bmatrix}, \qquad F_1 = \begin{bmatrix} c_{11} & c_{12} \\ p' - p's'c_{11} - q't'c_{11} & q' - p's'c_{11} - q't'c_{12} \end{bmatrix}.$$

Then, by (3.4)–(3.6) and Proposition 1.14, $AF = \begin{bmatrix} g_L & 0 \\ * & * \end{bmatrix}$, $F_1 = F^{-1}$. □

The above proof of Lemma 3.4 actually shows the construction of the desired matrices E and F. In general, the matrices E and F are not unique.

In the following theorem, we generalize the row and column operations denoted by E and F in Lemma 3.4 to those applied on a matrix of any size.

Theorem 3.2. *Let $A = (a_{ij}) \in \mathbb{M}_{m\times n}(S)$, $g_R = \mathrm{gcrd}(a_{11}, ..., a_{m1})$ and $g_L = \mathrm{gcld}(a_{11}, ..., a_{1n})$. Then there exist invertible matrices $E \in \mathbb{M}_m(S)$ and $F \in \mathbb{M}_m(S)$, such that*

$$EA = \begin{bmatrix} g_R & * \\ \underline{0} & * \end{bmatrix}, \qquad AF = \begin{bmatrix} g_L & \underline{0} \\ * & * \end{bmatrix},$$

where each $*$ stands for some matrix over S of suitable size and each $\underline{0}$ stands for a zero matrix of the appropriate size.

Proof. We first show the existence of E. If $m = 1$, then we have nothing to prove. If $m = 2$, then the existence of E is clear by Lemma 3.4. Suppose $m \geq 3$. By Lemma 3.4, there exists an invertible matrix $E_1 \in \mathbb{M}_2(S)$ such that

$$\begin{bmatrix} E_1 & \underline{0} \\ \underline{0} & I_{m-2} \end{bmatrix} A = \begin{bmatrix} \mathrm{gcrd}(a_{11}, a_{21}) & * & \cdots & * \\ 0 & * & \cdots & * \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

Let M be the $m \times m$ elementary matrix which corresponds to interchanging row 2 and row 3. Then by Lemma 3.4, there exists an invertible matrix $E_2 \in \mathbb{M}_2(S)$ such that

$$\begin{bmatrix} E_2 & \underline{0} \\ \underline{0} & I_{m-2} \end{bmatrix} M \begin{bmatrix} E_1 & \underline{0} \\ \underline{0} & I_{m-2} \end{bmatrix} A = \begin{bmatrix} \gcrd(a_{11}, a_{21}, a_{31}) & * & \cdots & * \\ 0 & * & \cdots & * \\ 0 & * & \cdots & * \\ a_{41} & a_{42} & \cdots & a_{4n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}.$$

By Lemma 3.4, $\begin{bmatrix} E_2 & \underline{0} \\ \underline{0} & I_{m-2} \end{bmatrix} M \begin{bmatrix} E_1 & \underline{0} \\ \underline{0} & I_{m-2} \end{bmatrix}$ is invetible over S. If we keep proceeding in the above way, we eventually get an invertible matrix $E \in \mathbb{M}_m(S)$, such that $EA = \begin{bmatrix} g_R & * \\ \underline{0} & * \end{bmatrix}$.

The existence of the matrix F can be shown analogously. □

Lemma 3.5. *Let* $A = \begin{bmatrix} 1 & \underline{0} \\ \underline{0} & B \end{bmatrix}$ *be a matrix over* S*, where* $B \in \mathbb{M}_{m\times n}(S)$*,* $m, n \in \mathbb{N}^+$ *and each* $\underline{0}$ *is a zero matrix of the appropriate size. Then* A *is regular over* S *if and only if* B *is regular over* S*. Moreover, if* $C \in \mathbb{M}_{n\times m}(S)$ *is a* $\{1\}$*-inverse of* B*, then* $\begin{bmatrix} 1 & \underline{0} \\ \underline{0} & C \end{bmatrix}$ *is a* $\{1\}$*-inverse of* A *over* S*.*

Proof. If A is regular over S, then by Theorem 3.1, B is regular over S. Conversely, suppose $C \in \mathbb{M}_{n\times m}(S)$ is a $\{1\}$-inverse of B, that is, $BCB = B$. Let $G = \begin{bmatrix} 1 & \underline{0} \\ \underline{0} & C \end{bmatrix}$. Then $AGA = \begin{bmatrix} 1 & \underline{0} \\ \underline{0} & BCB \end{bmatrix} = \begin{bmatrix} 1 & \underline{0} \\ \underline{0} & B \end{bmatrix} = A$, and so G is a $\{1\}$-inverse of A over S. Therefore, A is regular over S. □

3.2 Algorithm

We now introduce the algorithm for finding a $\{1\}$-inverse of a given matrix over the skew polynomial ring S.

Algorithm 5 Find a $\{1\}$-inverse of a given matrix over S

Input $A = (a_{ij}) \in \mathbb{M}_{m\times n}(S)$, where $m, n \in \mathbb{N}^+$.

Output $\begin{cases} G \in \mathbb{M}_{n\times m}(S) \text{ such that } AGA = A, \text{ if } A \text{ is regular} \\ \text{“Not regular.”, otherwise} \end{cases}$

1: $g_1 \leftarrow \text{gcrd}(a_{11}, a_{21}, ..., a_{m1})$, $g_2 \leftarrow \text{gcld}(a_{11}, a_{12}, ..., a_{1n})$

2: **for** i **from** 1 **to** 2 **do**

  if $g_i \in R$ **then** $h_i \leftarrow \begin{cases} g_i^{-1}, \text{ if } g_i \neq 0 \\ 0, \text{ otherwise} \end{cases}$ **end if**

3: **end for**

4: **if** $m = n = 1$ **then**

5: **if** $g_1 \in R$ **then return** $G \leftarrow [h_1]$ **else return** “Not regular.” **end if**

6: **else if** $m = 1$ **then**

  find an invertible matrix $F \in \mathbb{M}_{n\times n}(S)$ such that

  $AF = \begin{bmatrix} g_2 & 0_{1\times(n-1)} \end{bmatrix}$ (Theorem 3.2)

7: **if** $g_2 \in R$ **then return** $G \leftarrow F \begin{bmatrix} h_2 \\ 0_{(n-1)\times 1} \end{bmatrix}$ **else return** “Not regular.”

8: **end if**

9: **else if** $n = 1$ **then**

  find an invertible matrix $E \in \mathbb{M}_{m\times m}(S)$ such that

  $EA = \begin{bmatrix} g_1 \\ 0_{(m-1)\times 1} \end{bmatrix}$ (Theorem 3.2),

10: **if** $g_1 \in R$ **then return** $G \leftarrow \begin{bmatrix} h_1 & 0_{1\times(m-1)} \end{bmatrix} E$

11: **else return** “Not regular.”

12: **end if**

13: **else** find invertible matrices $E \in \mathbb{M}_{m\times m}(S)$ and $F \in \mathbb{M}_{n\times n}(S)$ such that

$$EA = \begin{bmatrix} g_1 & \underline{b} \\ 0_{(m-1)\times 1} & * \end{bmatrix}, (EA)F = \begin{bmatrix} g & 0_{1\times(n-1)} \\ * & B \end{bmatrix},$$

Algorithm 5 Find a $\{1\}$-inverse of a given matrix over S(continued)

where $\underline{b} = \begin{bmatrix} b_1 & \cdots & b_{n-1} \end{bmatrix}$, $g = \text{gcld}(g_1, b_1, ..., b_{n-1})$, and each $*$ denotes some matrix of the appropriate size (Theorem 3.2)

if $g \neq 1$ **then return** "Not regular." (Theorem 3.1)

else find an invertible matrix $M \in \mathbb{M}_{m\times m}(S)$ such that

$$M((EA)F) = \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix},$$

call Algorithm5 to compute a $\{1\}$-inverse H of B over S,

return $G \leftarrow F \begin{bmatrix} 1 & 0_{1\times(m-1)} \\ 0_{(n-1)\times 1} & H \end{bmatrix} ME$

end if

end if

Theorem 3.3. *In Algorithm 5, the $n \times m$ matrix G is a $\{1\}$-inverse of the $m \times n$ matrix A over the skew polynomial ring S.*

Proof. Let A, G, B, H g and h be as in Algorithm 5.

If $m = n = 1$, then $AGA = \begin{bmatrix} g_1 \end{bmatrix} \begin{bmatrix} h_1 \end{bmatrix} \begin{bmatrix} g_1 \end{bmatrix} = \begin{bmatrix} g_1 \end{bmatrix} = A$.

If $m = 1$, then

$$AGA = AF \begin{bmatrix} h_2 \\ 0_{(n-1)\times 1} \end{bmatrix} A = \begin{bmatrix} g_2 & 0_{1\times(n-1)} \end{bmatrix} \begin{bmatrix} h_2 \\ 0_{(n-1)\times 1} \end{bmatrix} A = A.$$

If $n = 1$, then

$$AGA = A \begin{bmatrix} h_1 & 0_{1\times(m-1)} \end{bmatrix} EA = A \begin{bmatrix} h_1 & 0_{1\times(m-1)} \end{bmatrix} \begin{bmatrix} g_1 \\ 0_{(m-1)\times 1} \end{bmatrix} = A.$$

If $m \geq 2,\ n \geq 2$, then $E_{m\times m}$, $F_{n\times n}$ $M_{m\times m}$ and $H_{(n-1)\times(m-1)}$ are such that

$$MEAF = \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix}, \qquad BHB = B,$$

which gives

$$
\begin{aligned}
MEAGAF &= MEAF \begin{bmatrix} 1 & 0_{1\times(m-1)} \\ 0_{(n-1)\times 1} & H \end{bmatrix} MEAF \\
&= \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix} \begin{bmatrix} 1 & 0_{1\times(m-1)} \\ 0_{(n-1)\times 1} & H \end{bmatrix} \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & BH \end{bmatrix} \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & BHB \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ 0_{(m-1)\times 1} & B \end{bmatrix} \\
&= MEAF.
\end{aligned}
$$

Since E, F and M are invertible over S (Theorem 3.2), we have $AGA = A$, which completes the proof. □

Example 3.2. *Let* $S = \mathbb{C}[x;\sigma]$ $(= \mathbb{C}[x;\sigma,0])$, *where* σ *is the standard complex conjugation on* $\mathbb{C}$. *Then* $\forall c \in \mathbb{C}$, $xc = \bar{c}x$. *Let* $A = \begin{bmatrix} 1 & ix & 0 \\ ix^2 & -x^3 - x^2 + 1 & x \end{bmatrix}$ *be a matrix over* S. *Then* $G = \begin{bmatrix} 1 + x^3 & -ix \\ -ix^2 & 1 \\ ix^3 & x \end{bmatrix}$ *is a* $\{1\}$*-inverse of* A *over* S.

Chapter 4

Other Results

In this chapter, we explore the properties of a variety of generalized inverses for matrices over the skew polynomial ring S.

4.1 Involutions on Skew Polynomial Rings

From Chapter 1 we know that the concept of an involution is needed when studying MP-inverses. The existence of an involution is known for some division rings (for example, the quaternion conjugation over the division ring of quaternions). In this section, we extend involutions on division rings to some particular skew polynomial rings in order to support our investigation on the skew polynomial ring $S = R[x; \sigma, \delta]$, where R is a division ring, σ is an automorphism of R and δ is a σ-derivation.

In this section, we let R be the division ring with an involution $f : \ r \mapsto \overline{r}$.

Proposition 4.1. *Suppose $\sigma = 1$ and $\delta(\overline{r}) = \overline{\delta(r)}$ for any $r \in R$. Define a function g*

$$\begin{array}{rccc} g: & S & \to & S \\ & \sum_{i=0}^{n} r_i x^i & \mapsto & \sum_{i=0}^{n} (-x)^i \overline{r_i} \end{array}, \ r_i \in R, \ i = 1, ..., n.$$

Then g is an involution over S.

Proof. Let $p = \sum_{i=0}^{m} a_i x^i,\ q = \sum_{j=0}^{n} b_j x^j$ be two arbitrary polynomials in S with $a_i, b_j \in R$. Clearly, $g(p) + g(q) = g(p+q)$. Let ax^s, bx^t $(a \neq 0,\ b \neq 0)$ denote the s^{th} term of p and the t^{th} term of q, respectively. Then, to show $g(pq) = g(q)g(p)$, it suffices to prove that $g(ax^s bx^t) = g(bx^t)g(ax^s)$ holds for any $s \in \{0, ..., m\}$ and $t \in \{0, ..., n\}$.

$$
\begin{aligned}
g(ax^s bx^t) &= g\left(a\left(\sum_{i=0}^{s}\binom{s}{i}\delta^{s-i}(b)x^i\right)x^t\right) && [\text{ Lemma 1.2 }]\\
&= \sum_{i=0}^{s} g\left(a\binom{s}{i}\delta^{s-i}(b)x^{t+i}\right)\\
&= \sum_{i=0}^{s}\binom{s}{i}(-x)^{t+i}\overline{a\delta^{s-i}(b)}\\
&= \sum_{i=0}^{s}(-1)^{t+i}\binom{s}{i}x^{t+i}\delta^{s-i}(\overline{b})\overline{a},\\
g(bx^t)g(ax^s) &= (-x)^t\overline{b}(-x)^s\overline{a}\\
&= (-1)^{t+s}x^t(\sum_{i=0}^{s}\binom{s}{i}(-1)^{s-i}x^i\delta^{s-i}(\overline{b}))\overline{a} && [\text{ Lemma 1.2 }]\\
&= \sum_{i=0}^{s}(-1)^{t+2s-i}\binom{s}{i}x^{t+i}\delta^{s-i}(\overline{b})\overline{a}\\
&= \sum_{i=0}^{s}(-1)^{t+i}\binom{s}{i}x^{t+i}\delta^{s-i}(\overline{b})\overline{a}.
\end{aligned}
$$

Thus, $g(ax^s bx^t) = g(bx^t)g(ax^s)$. One can easily verify that g is a bijection. So g is an anti-automophism. We now prove that g is of order 2. Since $g(p+q) = g(p) + g(q)$ for any $p, q \in S$, it suffices to show that $g(g(ax^n)) = ax^n$ for any $a \in R,\ n \in \mathbb{N}$.

$$
\begin{aligned}
g(g(ax^n)) &= g((-x)^n\overline{a})\\
&= (-1)^n g(\sum_{i=0}^{n}\binom{n}{i}\delta^{n-i}(\overline{a})x^i) && [\text{ Lemma 1.2}]\\
&= \sum_{i=0}^{n}(-1)^{n+i}\binom{n}{i}x^i\delta^{n-i}(a)\\
&= \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}x^i\delta^{n-i}(a)
\end{aligned}
$$

$$= ax^n \qquad [\text{ Lemma 1.2 }]$$

Hence g is of order 2 and so is an involution over S. □

Recall that for a ring P, the *centre* of P is

$$Z(P) = \{x \in P |\ xr = rx \text{ for all } r \in P\}.$$

Proposition 4.2. *Suppose $\sigma = 1$ and $\delta(\overline{r}) = \overline{\delta(r)}$ for any $r \in R$. Let $c \in Z(R)$ such that $c \neq 0$, $\delta(c) = 0$ and define a function g as follows*

$$\begin{array}{rccc} g: & S & \to & S \\ & \sum_{i=0}^{n} r_i x^i & \mapsto & \sum_{i=0}^{n} (cx)^i \overline{r_i} \end{array}, \ r_i \in R,\ i = 1, ..., n.$$

(a) If there exists some $a \in R \setminus \{0\}$ such that $\delta(a) \neq 0$, then g is an involution over S if and only if $c = -1$.

(b) If $\delta = 0$ and $c\overline{c} = 1$, then g is an involution over S.

(c) If $c \neq -1$ and g is an involution over S, then $\delta = 0$.

Proof. (a) Let $a \in R \setminus \{0\}$ be as above. Suppose g is an involution. Since $\sigma = 1$ and $\delta(c) = 0$, we have $xc = \sigma(c)x + \delta(c) = cx$. Let $p = x,\ q = ax$ be two elements of S. Then

$$\begin{aligned} g(pq) &= g(\sigma(a)x^2 + \delta(a)x) \\ &= g(ax^2) + g(\delta(a)x) \\ &= (cx)^2\overline{a} + cx\overline{\delta(a)} \\ &= x^2c^2\overline{a} + xc\delta(\overline{a}), \end{aligned} \qquad \begin{aligned} g(q)g(p) &= (cx)\overline{a}(cx) \\ &= c^2x\overline{a}x \\ &= c^2x(x\overline{a} - \delta(\overline{a})) \\ &= x^2c^2\overline{a} + x(-c^2\delta(\overline{a})). \end{aligned}$$

If g is an involution on S, then $g(pq) = g(q)g(p)$, and so $c\delta(\overline{a}) = -c^2\delta(\overline{a})$, i.e.,

$$(1 + c)c\delta(\overline{a}) = 0.$$

Since $c \neq 0$ and R has no zero divisor, we have either $\delta(\overline{a}) = 0$ or $(1+c) = 0$, i.e., $\overline{\delta(a)} = 0$ or $c = -1$. Since f is a bijection and $\delta(a) \neq 0$, we have $\overline{\delta(a)} \neq 0$. Hence $c = -1$.

Conversely, if $c = -1$, then by Proposition 4.1, g is an involution on S.

(b) Suppose $\delta = 0$. Then for all $r \in R$, $xr = \sigma(r)x + \delta(r) = rx$. Let $p = \sum_{i=0}^{m} a_i x^i$, $q = \sum_{j=0}^{n} b_j x^j$ be two arbitrary polynomials in S with $a_i, b_j \in R$. Clearly, $g(p) + g(q) = g(p+q)$. Let ax^s, bx^t $(a \neq 0,\ b \neq 0)$ denote the s^{th} term of p and the t^{th} term of q, respectively. Then, to show $g(pq) = g(q)g(p)$, it suffices to prove that $g(ax^s bx^t) = g(bx^t)g(ax^s)$ holds for any $s \in \{0, ..., m\}$ and $t \in \{0, ..., n\}$.

$$\begin{aligned} g(ax^s bx^t) &= g(abx^s x^t) & \qquad g(bx^t)g(ax^s) &= (cx)^t \overline{b}(cx)^s \overline{a} \\ &= (cx)^{s+t}\overline{ab} & &= c^t x^t \overline{b} c^s x^s \overline{a} \\ &= c^{s+t}x^{s+t}\overline{b}\overline{a}, & &= c^{t+s}x^{t+s}\overline{b}\overline{a}. \end{aligned}$$

Clear, $g(ax^s bx^t) = g(bx^t)g(ax^s)$. One can easily verify that g is a bijection. Therefore, g is an anti-automorphism on S.

We now prove that g is of order 2. Since g is a homomorphism of the additive group of S, it suffices to show that $g(g(ax^n)) = ax^n$ for any $a \in R,\ n \in \mathbb{N}$.

$$g(g(ax^n)) = g((cx)^n\overline{a}) = g(c^n\overline{a}x^n) = (cx)^n\overline{c^n\overline{a}} = a(c\overline{c})^n x^n = ax^n.$$

Hence g is of order 2 and so is an involution over S.

(c) Suppose $c \neq -1$ and g is an involution. Then for any $p, q \in S$, $g(pq) = g(q)g(p)$. Let a be an arbitrary element in $R \setminus \{0\}$. Set $p = x$ and $q = ax$. Then, by Part (a), $g(pq) = g(q)g(p)$ gives

$$(1+c)c\delta(\overline{a}) = 0.$$

Since $c \neq -1$, $c \neq 0$ and R has no zero divisor, we have $\delta(\overline{a}) = 0$, i.e., $\overline{\delta(a)} = 0$. By definition, f is a bijection. So $\delta(a) = 0$. Hence for all $r \in R$, $\delta(r) = 0$.

□

Recall that for an element c of R, the *conjugation by* c is the automorphism $h_c : \ r \to c^{-1}rc$ over R, where c^{-1} is the inverse of c in R.

From the above we see that involutions on skew polynomial rings exist when the skew polynomial rings satisfy some conditions. Thus, we can assume the existence of an involution on the skew polynomial ring S and use the involution to define generalized inverses for matrices over S.

4.2 Some Basic Properties

Recall that, given a matrix $A = (a_{ij})_{m\times n}$ over the skew polynomial ring $S = R[x; \sigma, \delta]$, where R is the skew field with an involution $a \to \overline{a}$ $(a \in R)$, the involution transpose of A over S is $A^* = (\overline{A})^T = (\overline{a_{ji}})_{n\times m}$. Let $B = (b_{ij})_{n\times k}$ be a matrix over S as well. Then by definition, we can verify the following identities without difficulty:

$$(\overline{A})^T = \overline{(A^T)},$$
$$(A^*)^{-1} = (A^{-1})^*.$$

Note that the following identities do not generally hold:

(a) $(AB)^T = B^T A^T$,

(b) $(\overline{A})(\overline{B}) = \overline{BA}$,

(c) $(A^{-1})^T = (A^T)^{-1}$,

(d) $\overline{(A^{-1})} = (\overline{A})^{-1}$.

For instance, let $A = \begin{bmatrix} a & a \\ 0 & b \end{bmatrix}$, $B = \begin{bmatrix} b & b \\ 0 & a \end{bmatrix}$, where $a, b \in S$ such that $ab \neq ba$. Then

$$(AB)^T = \begin{bmatrix} ab & 0 \\ ab + a^2 & ba \end{bmatrix} \neq \begin{bmatrix} ba & 0 \\ ba + a^2 & ab \end{bmatrix} = B^T A^T,$$

$$(\overline{A})(\overline{B}) = \begin{bmatrix} \overline{ba} & \overline{ba + a^2} \\ 0 & \overline{ab} \end{bmatrix} \neq \begin{bmatrix} \overline{ba} & \overline{ba + b^2} \\ 0 & \overline{ab} \end{bmatrix} = \overline{BA},$$

$$(A^{-1})^T A^T \neq (AA^{-1})^T = I^T = I, \text{ that is, } (A^{-1})^T \neq (A^T)^{-1},$$

$$\overline{(A^{-1})}(\overline{A}) \neq \overline{A^{-1}A} = \overline{I} = I, \text{ that is, } \overline{(A^{-1})} \neq (\overline{A})^{-1}.$$

In Section 1.5.2 we gave the definition of the rank of a matrix over S. We now give a property of matrices of left (right, resp.) full rank as follows.

Lemma 4.1. *Let $A_{m\times n}$ be a matrix over S. Suppose $\rho(A) = m$, $1 \leq m \leq n$. Then A has a right inverse over $Q(S)$. Similarly, A has a left inverse over $Q(S)$ if $\rho(A) = n$, $1 \leq n \leq m$.*

Proof. We shall only prove the result for the case $\rho(A) = m$. The case $\rho(A) = n$ can be shown analogously.

By Proposition 1.12 and Theorem 3.2, there exists an $n \times n$ matrix F over $Q(S)$, such that

$$AF = \begin{bmatrix} 1 & 0_{1\times(n-1)} \\ * & * \end{bmatrix},$$

where each $*$ denotes some matrix of the appropriate size. Since $\rho(A) = m$, by using the above method, we can find a $n \times n$ matrix B_1 over $Q(S)$, such that

$$AB_1 = \begin{cases} \begin{bmatrix} I_m & 0_{m\times(n-m)} \end{bmatrix}, & \text{if } m < n \\ I_m, & \text{if } m = n \end{cases}.$$

Let

$$B_2 = \begin{cases} \begin{bmatrix} I_m \\ 0_{(n-m)\times m} \end{bmatrix}, \text{ if } m < n \\ I_m, \text{ if } m = n \end{cases},$$

and $B = B_1 B_2$. Then $AB = I_m$, and so A has a right inverse over $Q(S)$. □

4.3 Matrix Diagonalization

Matrix Diagonalization is very useful when studying properties of matrices. Over a commutative PID, every square matrix can be changed into a particular diagonal matrix, by the Smith normal form theorem ([30], Theorem 4.10). In non-commutative case, we have some similar results.

In this section, we show that every matrix (not necessary square) over the skew polynomial ring S can be converted into a diagonal matrix that has the same fundamental properties of the underlying matrix in order to support our further investigation on the generalized inverses for matrices over S.

Proposition 4.3. *Let $A \in \mathbb{M}_{m\times n}(S) \setminus \{\underline{0}\}$ such that $\rho(A) = r$. Then there exist invertible matrices $U \in \mathbb{M}_{m\times m}(S)$ and $V \in \mathbb{M}_{n\times n}(S)$ such that*

$$UAV = \left[\begin{array}{cccc|cc} x_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & x_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x_r & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{array}\right], \tag{4.1}$$

where $x_1, x_2, ..., x_r$ are nonzero elements in S.

Proof. We first prove the following

Claim. The matrix A can be converted into an $m \times n$ matrix of the form

$$\begin{bmatrix} * & \underline{0} \\ \underline{0} & D \end{bmatrix}, \tag{4.2}$$

where $*$ denotes some element in S and each $\underline{0}$ denotes a zero matrix of the appropriate size, by performing elementary row and column operations.

Let $A_1 = A$. Suppose $A_1(s,t)$ is a nonzero entry that is of the lowest degree in A_1. Then there exist invertible matrices $E_1 \in \mathbb{M}_{m\times m}(S)$ and $F_1 \in \mathbb{M}_{n\times n}(S)$ such that $E_1A_1F_1 = A_2$, where $A_2(1,1) = A_1(s,t)$. Suppose $b_1 = \text{gcrd}(A_2(1,1), ..., A_2(m,1))$. By Theorem 3.2, there exists an invertible matrix $E_2 \in \mathbb{M}_{m\times m}(S)$, such that

$$E_2A_2 = B = \begin{bmatrix} b_1 & b_2 & \cdots & b_n \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{bmatrix}, \ b_2, ..., b_n \in S.$$

If $\text{gcld}(b_1, b_2, ..., b_n) = b_1$, then there exists an invertible matrix $F_2 \in \mathbb{M}_{n\times n}(S)$ such that

$$BF_2 = \begin{bmatrix} b_1 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{bmatrix}.$$

If $\text{gcld}(b_1, b_2, ..., b_n) = 1 \neq b_1$, then by Theorem 3.2, there exists an invertible matrix $F_2 \in \mathbb{M}_{n\times n}(S)$ such that

$$BF_2 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{bmatrix},$$

and so there exists an invertible matrix $E_3 \in \mathbb{M}_{m\times m}(S)$, such that E_3BF_2 is of the form (4.2).

If $\text{gcld}(b_1, b_2, ..., b_n) = c_1$, where $c_1 \neq 1$ and $c_1 \neq b_i$ for $i = 1, 2, ..., n$, then $\deg(c_1) < \deg(b_1) \leq \deg(A_2(1,1)) \leq \deg(A_1(1,1))$. By Theorem 3.2, there exists an invertible matrix $F_2 \in \mathbb{M}_{n\times n}(S)$ such that

$$BF_2 = C = \begin{bmatrix} c_1 & 0 & \cdots & 0 \\ c_2 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ c_m & * & \cdots & * \end{bmatrix}, \ c_2, ..., c_m \in S.$$

If $\text{gcrd}(c_1, c_2, ..., c_m) = c_1$ or $\text{gcrd}(c_1, c_2, ..., c_m) = 1$, then the claim is clear. Otherwise, we let $A_1 = C$ and repeat the above process.

Since $\deg(A_1(1,1))$ strictly decreases in each iteration, we eventually get a matrix B such that $\text{gcld}(b_1, b_2, ..., b_n) = b_1$ or $\text{gcld}(b_1, b_2, ..., b_n) = 1$ (or a matrix C such that $\text{gcrd}(c_1, c_2, ..., c_m) = c_1$ or $\text{gcrd}(c_1, c_2, ..., c_m) = 1$). Thus, we can convert B (or C) into a matrix of the form (4.2) by applying elementary column (or row) operations.

After we convert A into the form (4.2), we let $A_1 = D$ and repeat the above process. Since $\rho(A) = r$, we eventually convert A into the form (4.1). Therefore, there exist invertible matrices $U \in \mathbb{M}_{m\times m}(S)$ and $V \in \mathbb{M}_{n\times n}(S)$ such that UAV is of the form (4.1).

□

4.4 $\{1\}$-inverses

Recall that a matrix A over the skew polynomial ring S is called a regular matrix if there exists some matrix G over S such that

$$AGA = A.$$

In this case, G is called a $\{1\}$-inverse of A, written A^-.

In Section 1.5.2 we gave the definition of the rank of an $m \times n$ matrix A, written $\rho(A)$, over the skew polynomial ring S. In this section, we shall explore the relation of the rank of a matrix to the existence of a $\{1\}$-inverse of the matrix over S.

Proposition 4.4. *Let $A_{m\times n}$, $G_{n\times m}$ be two matrices over S.*

(a) If $AGA = A$, then $\rho(A) \leq \rho(G)$.

(b) If $AGA = A$ and $GAG = G$, then $\rho(A) = \rho(G)$.

Proof. By (1.18). □

We now give a result that can be used to determine the existence of a $\{1\}$-inverse of a matrix over S.

Proposition 4.5. *Let A be an $m \times n$ matrix over S such that $\rho(A) = m$ ($\rho(A) = n$, resp.). Then a matrix G over S is a $\{1\}$-inverse of A if and only if G is a right (left, resp.) inverse of A over S.*

Proof. We shall only prove the result for the case $\rho(A) = m$. The case $\rho(A) = n$ can be shown analogously.

Suppose that G is a $\{1\}$-inverse of A over S. Consider $A_{m\times n}$ as a matrix over $Q(S)$. Since $\rho(A) = m$, A has a right inverse over $Q(S)$, by Lemma 4.1. Let B denote a right inverse of A over $Q(S)$. Then $AG = AGAB = AB = I$, and so G is a right inverse of A over S. Conversely, if G is a right inverse of A over S, then $AGA = IA = A$, and so G is a $\{1\}$-inverse of A. □

In Section 1.5.2 we gave the definition of rank factorization for a matrix over S. We now give an alternative definition of rank factorization as follows.

Proposition 4.6. *Given any $m \times n$ matrix A over S, where $m, n \in \mathbb{N}$. Let $A = B_{m\times r}C_{r\times n}$ be a decomposition of A over the Ore quotient ring $Q(S)$ of S, where $r \in \mathbb{N}$. The following are equivalent.*

(a) $A = BC$ is a rank factorization of A over S, i.e., $\rho(A) = r$.

(b) $\rho(B) = r$, $\rho(C) = r$.

(c) B has a left inverse and C has a right inverse over the Ore quotient ring $Q(S)$ of S.

Proof. (a) $\Rightarrow$ (b). Suppose $\rho(A) = r$. Note that $r \leq \min\{m, n\}$. By (1.15) and (1.18), $\rho(B) = r$, $\rho(C) = r$.

(b) $\Rightarrow$ (c). Suppose $\rho(B) = r$, $\rho(C) = r$. By Lemma 4.1, B has a left inverse and C has a right inverse over $Q(S)$.

(c) $\Rightarrow$ (a). Suppose B has a left inverse $B^{-1}_{r\times m}$ and C has a right inverse $C^{-1}_{n\times r}$ over $Q(S)$. Then $B^{-1}AC^{-1} = I_r$. By (1.18), $\rho(A) \geq \rho(I_r) = r$. On the other hand, $\rho(A) \leq r$, by the definition of inner rank. Thus, $\rho(A) = r$. □

4.5 $\{1,2\}$-inverses

Given a matrix A over the skew polynomial ring S, a matrix G over S is called a $\{1,2\}$-inverse of A if

$$AGA = A,$$
$$GAG = G.$$

We have seen that, for any matrix A over S, there exist invertible matrices U and V over S such that UAV is a diagonal matrix that shares the same fundamental properties with A (Proposition 4.3). In this section, we shall use this property to investigate the $\{1,2\}$-inverses of matrices over S.

Theorem 4.1. *Let A be a regular matrix over S.*

(a) Suppose $A = U \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} V$ for some invertible matrices U and V over S. A matrix of the form

$$V^{-1} \begin{bmatrix} I & B \\ C & CB \end{bmatrix} U^{-1} \tag{4.3}$$

for some matrices B, C of appropriate size is a $\{1,2\}$-inverse of A. Moreover, every $\{1,2\}$-inverse of A can be expressed in the form of (4.3).

(b) Suppose A has a rank factorization $A = A_L A_R$ such that A_L has a left inverse A_L^{-1} and A_R has a right inverse A_R^{-1} over S. The matrix $A_R^{-1} A_L^{-1}$ is a $\{1,2\}$-inverse of A. Moreover, every $\{1,2\}$-inverse of A can be expressed in the form $A_R^{-1} A_L^{-1}$.

Proof. (a) By definition, one can verify that $V^{-1} \begin{bmatrix} I & B \\ C & CB \end{bmatrix} U^{-1}$ is a $\{1,2\}$-inverse of $U \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} V$ with out difficulty.

On the other hand, if a matrix G over S is a $\{1,2\}$-inverse of $U \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} V$, namely,

$$U \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} VGU \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} V = U \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} V, \quad GU \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} VG = G,$$

then we have

$$\begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} VGU \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} = \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix}, \quad VGU \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} VGU = VGU,$$

since U are V are invertible over S. This gives that VGU is a $\{1,2\}$-inverse

of $\begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix}$ over S. Without loss of generality, suppose $VGU = \begin{bmatrix} E & B \\ C & D \end{bmatrix}$ for some matrices E, B, C, D of appropriate size. Then

$$\begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} \begin{bmatrix} E & B \\ C & D \end{bmatrix} \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} = \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix}, \quad \begin{bmatrix} E & B \\ C & D \end{bmatrix} \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} \begin{bmatrix} E & B \\ C & D \end{bmatrix} = \begin{bmatrix} E & B \\ C & D \end{bmatrix},$$

that is,

$$\begin{bmatrix} E & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix} = \begin{bmatrix} I & \underline{0} \\ \underline{0} & \underline{0} \end{bmatrix}, \quad \begin{bmatrix} E^2 & EB \\ CE & CB \end{bmatrix} = \begin{bmatrix} E & B \\ C & D \end{bmatrix},$$

which implies that $E = I$, $D = CB$. Therefore, $VGU = \begin{bmatrix} I & B \\ C & CB \end{bmatrix}$, and so $G = V^{-1} \begin{bmatrix} I & B \\ C & CB \end{bmatrix} U^{-1}$.

(b) By definition, one can easily verify that $A_R^{-1}A_L^{-1}$ is a $\{1,2\}$-inverse of A_LA_R.

On the other hand, let G be a $\{1,2\}$-inverse of A_LA_R over S. Then

$$A_LA_RGA_LA_R = A_LA_R, \tag{4.4}$$

$$GA_LA_RG = G. \tag{4.5}$$

Since A_L has a left inverse A_L^{-1} over S and A_R has a right inverse A_R^{-1} over S, we get

$$GA_L = A_R^{-1}, \quad A_RG = A_L^{-1} \tag{4.6}$$

from (4.4). Substitute (4.6) into (4.5), we get $G = A_R^{-1}A_L^{-1}$.

□

Theorem 4.2. *Let A be a matrix over S. If G is a $\{1,2\}$-inverse of A over S,*

then every $\{1,2\}$*-inverse of* A *can be expressed in the form*

$$f_G(X,Y) = G + (I - GA)XAG + GAY(I - AG) + (I - GA)XAY(I - AG)$$

for some matrices X, Y *of appropriate size. In addition, every matrix of the form* $f_G(X,Y)$ *in which* G *is a* $\{1,2\}$*-inverse of* A *over* S *is also a* $\{1,2\}$*-inverse of* A *over* S*.*

Proof. Suppose G is a $\{1,2\}$-inverse of A. One can easily verify that $G = f_G(G,G)$. On the other hand, let X, Y be matrices of suitable size over S. One can verify that $Af_G(X,Y)A = A$, $f_G(X,Y)Af_G(X,Y) = f_G(X,Y)$ without difficulty. Thus, $f_G(X,Y)$ is a $\{1,2\}$-inverse of A over S □

4.6 MP-inverses

Given a matrix A over the skew polynomial ring S, a matrix G is said to be the MP-inverse of A over S, denoted by A^+, if

$$AGA = A,$$
$$GAG = G,$$
$$(AG)^* = AG,$$
$$(GA)^* = GA.$$

In this section, we investigate the existence and construction of MP-inverses of matrices over the skew polynomial ring S.

Recall that for any invertible matrices A and B over S, we have $(A^{-1})^* = (A^*)^{-1}$ and $(AB)^{-1} = B^{-1}A^{-1}$. Using these two identities, we can get the following identities:

$$(A^*A)^{-1} = ((A^*A)^{-1})^*, \tag{4.7}$$
$$(AA^*)^{-1} = ((AA^*)^{-1})^*. \tag{4.8}$$

We now introduce theorems used to determine the existence of MP-inverses of matrices over S.

Theorem 4.3. *Let A be an $m \times n$ matrix over the skew polynomial ring S with an involution $a \to \bar{a}$ such that $m \geq n$ and $\rho(A) = n$ ($m \leq n$ and $\rho(A) = m$, resp.). Then A has a MP-inverse if and only if A^*A (AA^*, resp.) is invertible. If A^*A (AA^*, resp.) is invertible, then $G := (A^*A)^{-1}A^*$ ($G := A^*(AA^*)^{-1}$, resp.) is the MP-inverse of A, and GG^* (G^*G, resp.) is the inverse of A^*A (AA^*, resp.) over S.*

Proof. We shall only prove the case in which $m \geq n$. The case in which $m \leq n$ can be shown analogously.

Suppose A has a MP-inverse G over S. Since $\rho(A) = n$, A has a left inverse A_L over $Q(S)$. Then $AGA = A$ implies

$$GA = I.$$

Also, $AGA = A$ together with $(AG)^* = AG$ give $(AG)^*A = A$, hence

$$G^*A^*A = A.$$

Thus, $GG^*A^*A = GA = I$, that is, A^*A has a left inverse GG^* over S. By Proposition 1.14, A^*A is invertible, and GG^* is the inverse of A^*A over S.

Conversely, suppose A^*A is invertible. We verify that $G := (A^*A)^{-1}A^*$ is the MP-inverse of A over S. Since $GA = (A^*A)^{-1}A^*A = I$, we have $AGA = A$, $GAG = G$ and $(GA)^* = GA$. Moreover, by (4.7), we have

$$\begin{aligned}(AG)^* = G^*A^* &= ((A^*A)^{-1}A^*)^*A^* = A((A^*A)^{-1})^*A^* \\ &= A(A^*A)^{-1}A^* = AG.\end{aligned}$$

Therefore, $G := (A^*A)^{-1}A^*$ is the MP-inverse of A over S. □

Theorem 4.4. *Let A be an $m \times n$ matrix over the skew polynomial ring S with an involution $a \to \bar{a}$. Let $\rho(A) = r$. Let $A = A_L A_R$, where A_L is an $m \times r$ matrix and A_R is a $r \times n$ matrix. Then the following are equivalent.*

(i) The MP-inverse A^+ of A over S exists.

(ii) The MP-inverse A_L^+ of A_L and the MP-inverse A_R^+ of A_R over S exist.

(iii) $A_L^* A_L$ and $A_R A_R^*$ are invertible.

Proof. $(i) \Rightarrow (ii)$. Suppose (i) holds, that is,

$$A_L A_R A^+ A_L A_R = A_L A_R, \tag{4.9}$$

$$A^+ A_L A_R A^+ = A^+, \tag{4.10}$$

$$(A_L A_R A^+)^* = A_L A_R A^+, \tag{4.11}$$

$$(A^+ A_L A_R)^* = A^+ A_L A_R. \tag{4.12}$$

We shall only show that $A_R A^+$ is the MP-inverse of A_L. The case of the MP-inverse of A_R can be shown analogously.

By (1.15) and (1.18), $\rho(A_L) = r$, $\rho(A_R) = r$. Thus, A_L has a left inverse A_L^{-1} and A_R has a right inverse A_R^{-1} over $Q(S)$. Then from (4.9) and (4.10) we get

$$A_L(A_R A^+)A_L = A_L, \tag{4.13}$$

$$(A_R A^+)A_L(A_R A^+) = A_R A^+. \tag{4.14}$$

Moreover, by (4.13), we have

$$\begin{aligned} A_R A^+ A_L &= (A_L^{-1} A_L) A_R A^+ A_L (A_R A_R^{-1}) \\ &= A_L^{-1}(A_L A_R A^+ A_L) A_R A_R^{-1} \\ &= A_L^{-1} A_L A_R A_R^{-1} \\ &= I, \end{aligned}$$

and so

$$A_R A^+ A_L = (A_R A^+ A_L)^*. \tag{4.15}$$

Hence, by (4.11), (4.13), (4.14) and (4.15), $A_R A^+$ is the MP-inverse of A_L over S.

$(ii) \Rightarrow (i)$. Suppose (ii) holds. Then

$$\begin{aligned} AA_R^+A_L^+A &= A_LA_RA_R^+A_L^+A_LA_R \\ &= A_LA_RA_R^+(A_RA_R^{-1}A_L^{-1}A_L)A_L^+A_LA_R \\ &= A_LA_RA_R^{-1}A_L^{-1}A_LA_R \\ &= A_LA_R \\ &= A, \end{aligned}$$

$$\begin{aligned} A_R^+A_L^+AA_R^+A_L^+ &= A_R^+A_L^+A_LA_RA_R^+A_L^+ \\ &= A_R^+(A_L^{-1}A_L)A_L^+A_LA_RA_R^+(A_RA_R^{-1})A_L^+ \\ &= A_R^+A_L^{-1}A_LA_RA_R^{-1}A_L^+ \\ &= A_R^+A_L^+, \end{aligned}$$

$$\begin{aligned} AA_R^+A_L^+ &= A_LA_RA_R^+A_L^+ \\ &= A_LA_RA_R^+(A_RA_R^{-1})A_L^+ \\ &= A_LA_RA_R^{-1}A_L^+ \\ &= A_LA_L^+ \\ &= (A_LA_L^+)^* \\ &= (AA_R^+A_L^+)^*, \end{aligned}$$

$$\begin{aligned} A_R^+A_L^+A &= A_R^+A_L^+A_LA_R \\ &= A_R^+(A_L^{-1}A_L)A_L^+A_LA_R \\ &= A_R^+A_L^{-1}A_LA_R \\ &= A_R^+A_R \\ &= (A_R^+A_R)^* \\ &= (A_R^+A_L^+A)^*. \end{aligned}$$

By definition, $A_R^+A_L^+$ is the MP-inverse of A.

$(ii) \Leftrightarrow (iii)$ follows from Theorem 4.3. □

Theorem 4.5. *Let A be an $m \times n$ matrix over the skew polynomial ring S with an involution $f:\ a \to \overline{a}$. If*

(a) $\rho(A^*A) = \rho(AA^*) = \rho(A)$ and

(b) A^*A and AA^* are regular over S,

then $H = A^*(AA^*)^-A(A^*A)^-A^*$ is the MP-inverse of A, where $(AA^*)^-$ and $(A^*A)^-$ are $\{1\}$-inverses of AA^* and A^*A, respectively.

Proof. Consider A, A^*A and AA^* as matrices over $Q(S)$. Since $\rho(A^*A) = \rho(A)$, there exists an unimodular matrix B over $Q(S)$ such that $BA^*A = A$. Also, since $\rho(A) = \rho(AA^*)$, there exists an unimodular matrix C over $Q(S)$ such that $AA^*C = A$. Hence

$$\begin{aligned} AHA &= AA^*(AA^*)^-A(A^*A)^-A^*A \\ &= AA^*(AA^*)^-BA^*A(A^*A)^-A^*A \\ &= AA^*(AA^*)^-BA^*A \\ &= AA^*(AA^*)^-A \\ &= AA^*(AA^*)^-AA^*C \\ &= AA^*C \\ &= A, \end{aligned}$$

$$\begin{aligned}
HAH &= A^*(AA^*)^-A(A^*A)^-A^*AA^*(AA^*)^-A(A^*A)^-A^* \\
&= A^*(AA^*)^-BA^*A(A^*A)^-A^*AA^*(AA^*)^-AA^*C(A^*A)^-A^* \\
&= A^*(AA^*)^-BA^*AA^*(AA^*)^-AA^*C(A^*A)^-A^* \\
&= A^*(AA^*)^-BA^*AA^*C(A^*A)^-A^* \\
&= A^*(AA^*)^-A(A^*A)^-A^* \\
&= H,
\end{aligned}$$

$$\begin{aligned}
(AH)^* &= (AA^*(AA^*)^-A(A^*A)^-A^*)^* \\
&= (AA^*(AA^*)^-AA^*C(A^*A)^-A^*)^* \\
&= (AA^*C(A^*A)^-A^*)^* \\
&= (A(A^*A)^-A^*)^* \\
&= (BA^*A(A^*A)^-(BA^*A)^*)^* \\
&= (BA^*A(A^*A)^-A^*AB^*)^* \\
&= (BA^*AB^*)^* \\
&= BA^*AB^* \\
&= AH,
\end{aligned}$$

$$\begin{aligned}
(HA)^* &= (A^*(AA^*)^-A(A^*A)^-A^*A)^* \\
&= (A^*(AA^*)^-BA^*A(A^*A)^-A^*A)^* \\
&= (A^*(AA^*)^-BA^*A)^* \\
&= (A^*(AA^*)^-A)^* \\
&= ((AA^*C)^*(AA^*)^-AA^*C)^* \\
&= (C^*AA^*(AA^*)^-AA^*C)^* \\
&= (C^*AA^*C)^* \\
&= C^*AA^*C \\
&= HA.
\end{aligned}$$

Thus H is the MP-inverse of A over S.

□

4.6.1 {1}-inverses of the Form PCQ

In Theorem 4.5 of the previous section, we saw that if a given matrix A over the skew polynomial ring S has an MP-inverse, then the MP-inverse of A can be expressed in the form of A^*CA^* for some matrix C over S, or, in other words, in the form of PCQ, where P and Q are given matrices over S. Since the MP-inverse is a special kind of {1}-inverse, we investigate whether a given matrix over S has a {1}-inverse of such form.

Theorem 4.6. *Let $A_{m\times n}$, $P_{n\times k}$ and $Q_{l\times m}$ be matrices over the skew polynomial ring S.*

(a) If $C_{k\times l}$ is a matrix over S, then PCQ is a {1}-inverse of A if and only if

(i) $\rho(QAP) = \rho(A)$,

(ii) C is a {1}-inverse of QAP over S.

(b) For some matrix $C_{k\times l}$, A has a {1}-inverse of the form PCQ if and only if

(i) $\rho(QAP) = \rho(A)$,

(ii) QAP is regular.

Moreover, if $\rho(P) = \rho(Q) = \rho(A)$ and A has a {1}-inverse of the form PCQ, then this {1}-inverse of A is unique.

Proof. (a) If PCQ is a {1}-inverse of A over S, that is,

$$APCQA = A, \tag{4.16}$$

then $APCQAPCQA = A$. By (1.18),

$$\rho(A) = \rho((APC)(QAP)(CQA)) \leq \rho(QAP), \quad \rho(QAP) \leq \rho(A),$$

so $\rho(QAP) = \rho(A)$. Also, By (4.16), $QAPCQAP = QAP$. Thus C is a $\{1\}$-inverse of QAP over S.

Conversely, suppose (i) and (ii) of Part (a) hold. By (1.18),

$$\rho(QAP) \leq \rho(QA) \leq \rho(A), \quad \rho(QAP) \leq \rho(AP) \leq \rho(A).$$

By assumption $\rho(QAP) = \rho(A)$, so we get

$$\rho(QA) = \rho(A) = \rho(AP).$$

Consider QA, AP, A as matrices over $Q(S)$. Since $\rho(QA) = \rho(A)$, $\rho(AP) = \rho(A)$, there exist matrices D and E over $Q(S)$ such that

$$DQA = A, \tag{4.17}$$

$$APE = A. \tag{4.18}$$

Since C is a $\{1\}$-inverse of QAP, namely, $QAPCQAP = QAP$, we have

$$DQAPCQAPE = DQAPE,$$

By (4.17) and (4.18), $APCQA = A$, that is, PCQ is a $\{1\}$-inverse of A.

(b) Follows from Part (a).

Now, let $\rho(P) = \rho(Q) = \rho(A)$. Suppose that A has a $\{1\}$-inverse of the form PCQ for some matrix C over S. By Part (a), $\rho(QAP) = \rho(A)$, which implies $\rho(P) = \rho(Q) = \rho(QAP)$. Consider Q, P, QAP as matrices over $Q(S)$. Then there exist matrices D and E over $Q(S)$ such that

$$E(QAP) = P, \tag{4.19}$$

$$(QAP)D = Q. \tag{4.20}$$

By (4.19),(4.20),

$$\begin{aligned} PCQ &= (EQAP)C(QAPD) \\ &= EQ(APCQA)PD \\ &= EQAPD \\ &= EQ \text{ (or } PD). \end{aligned}$$

This implies that the matrix PCQ is in fact independent of C. Also, from (4.19) and (4.20) we can see that E and Q are dependent on P and Q. Therefore, the matrix PCQ is unique. □

Theorem 4.6 outlines the sufficient and necessary conditions for a matrix to have a $\{1\}$-inverse of the form PCQ. Using this result, we can get the following conclusions without difficulty.

Corollory 4.1. *Let A be an $m \times n$ matrix over the skew polynomial ring S.*

(a) If C is a $n \times n$ matrix over S (D is a $m \times m$ matrix over S, resp.), then CA^* (A^*D, resp.) is a $\{1\}$-inverse of A if and only if

(i) $\rho(A^*A) = \rho(A)$ ($\rho(AA^*) = \rho(A)$, resp.),

(ii) C (D, resp.) is a $\{1\}$-inverse of A^*A (AA^*, resp.) over S.

(b) For some $n \times n$ matrix C (some $m \times m$ matrix D, resp.), A has a $\{1\}$-inverse of the form CA^* (A^*D, resp.) if and only if

(i) $\rho(A^*A) = \rho(A)$ ($\rho(AA^*) = \rho(A)$, resp.),

(ii) A^*A (AA^*, resp.) is regular.

Proof. The result for matrices of the form CA^* is obtained by taking $P = I, Q = A^*$ in Theorem 4.6. The result for matrices of the form A^*D can be shown analogously. □

Corollory 4.2. *Let A be an $m \times n$ matrix over S.*

(a) *If C is a $m \times n$ matrix over S, then A^*CA^* is a $\{1\}$-inverse of A if and only if*

(i) $\rho(A^*AA^*) = \rho(A)$,

(ii) *C is a $\{1\}$-inverse of A^*AA^* over S.*

(b) *For some $m \times n$ matrix C, A has a $\{1\}$-inverse of the form A^*CA^* if and only if*

(i) $\rho(A^*AA^*) = \rho(A)$,

(ii) *A^*AA^* is regular.*

Proof. The result is obtained by taking $P = A^*, Q = A^*$ in Theorem 4.6. □

Corollory 4.3. *Let A be an $m \times m$ matrix over S.*

(a) *If C is a $m \times m$ matrix over S, then AC (CA, resp.) is a $\{1\}$-inverse of A if and only if*

(i) $\rho(A^2) = \rho(A)$,

(ii) *C is a $\{1\}$-inverse of A^2 over S.*

(b) *For some $m \times m$ matrix C, A has a $\{1\}$-inverse of the form AC (CA, resp.) if and only if*

(i) $\rho(A^2) = \rho(A)$,

(ii) *A^2 is regular.*

Consequently, AC is a $\{1\}$-inverse of A if and only if CA is a $\{1\}$-inverse of A.

Proof. The result for matrices of the form AC is obtained by taking $P = A, Q = I$ in Theorem 4.6. The result for matrices of the form CA can be shown analogously.

□

Corollory 4.4. *Let A be an $m \times m$ matrix over S.*

(a) If C is a $m \times m$ matrix over S, then ACA is a $\{1\}$-inverse of A if and only if

(i) $\rho(A^3) = \rho(A)$,

(ii) C is a $\{1\}$-inverse of A^3 over S.

(b) For some $m \times m$ matrix C, A has a $\{1\}$-inverse of the form ACA if and only if

(i) $\rho(A^3) = \rho(A)$,

(ii) A^3 is regular.

Further, if A has a $\{1\}$-inverse of the form ACA, then the $\{1\}$-inverse of the form ACA of A is unique.

Proof. The result is obtained by taking $P = A, Q = A$ in Theorem 4.6. □

Corollory 4.5. *Let $A_{m\times m}$ be a matrix over S, $m \in \mathbb{N}$. The following statements are equivalent.*

(i) A has a $\{1\}$-inverse of the form AC for some matrix C over S.

(ii) A has a $\{1\}$-inverse of the form CA for some matrix C over S.

(iii) $\rho(A) = \rho(A^2)$ and A^2 is regular.

(iv) A has a $\{1\}$-inverse of the form ACA for some matrix C over S.

(v) $\rho(A) = \rho(A^3)$ and A^3 is regular.

(vi) $\rho(A) = \rho(A^n)$ and A^n is regular for $n \in \mathbb{N},\ n \geq 2$.

Proof. $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$. By Corollary 4.3.

$(iv) \Leftrightarrow (v)$. By Corollary 4.4.

To show $(iii) \Leftrightarrow (v)$, it suffices to show $(iii) \Leftrightarrow (vi)$.

$(iii) \Rightarrow (vi)$. Suppose (iii) holds. Since $\rho(A) = \rho(A^2)$, there exists a matrix B over $Q(S)$ such that $A^2B = A$. This gives

$$A = A^2B = A(A^2B)B = A^3B^2 = \cdots = A^nB^{n-1}. \tag{4.21}$$

By (1.18), $\rho(A) = \rho(A^nB^{n-1}) \leq \rho(A^n)$, $\rho(A^n) \leq \rho(A)$. Therefore, $\rho(A) = \rho(A^n)$.

On the other hand, let G be a $\{1\}$-inverse of A^2, that is, $A^2GA^2 = A^2$. By (4.21), $A^2GA = A^2GA^2B = A^2B = A$. Thus

$$A^n(GA)^{n-1} = A^{n-2}A^2GA(GA)^{n-2} = A^{n-2}A(GA)^{n-2} = \cdots = A,$$

and so

$$A^n = AA^{n-1} = A^n(GA)^{n-1}A^{n-1} = A^n(GA)^{n-2}GA^n,$$

that is, $(GA)^{n-2}G$ is a $\{1\}$-inverse of A^n over S.

To show $(vi) \Rightarrow (iii)$, it suffices to show $(vi) \Rightarrow (i)$. Suppose (vi) holds. Let G be a $\{1\}$-inverse of A^n. Since $\rho(A) = \rho(A^n)$, there exists a matrix B over $Q(S)$ such that $A^nB = A$. Since $A^nGA^n = A^n$, we have $A^nGA = A^nGA^nB = A^nB = A$, i.e.,

$$A(A^{n-1}G)A = A.$$

Therefore, A has a $\{1\}$-inverse of the form AC over S. □

4.7 $\{1,2,3\}$-inverses and $\{1,2,4\}$-inverses

Let $A_{m\times n}$ and $G_{n\times m}$ be two matrices over the skew polynomial ring S. Recall that G is called a $\{1,2,3\}$-inverse ($\{1,2,4\}$-inverse, resp.) of A if

$$AGA = A,$$
$$GAG = G,$$
$$(AG)^* = AG \ ((GA)^* = GA, \text{ resp.}).$$

In this section, we shall investigate the existence and construction of $\{1,2,3\}$-inverses and $\{1,2,4\}$-inverses of matrices over the skew polynomial ring S.

Proposition 4.7. *Let A be an $m \times n$ matrix over S. Then*

(a) A $\{1\}$-inverse G of A is a $\{1,2,3\}$-inverse of A if and only if G is of the form CA^* for some matrix C over S.

(b) A $\{1\}$-inverse G of A is a $\{1,2,4\}$-inverse of A if and only if G is of the form A^*C for some matrix C over S.

(c) A $\{1\}$-inverse G of A is the MP-inverse of A if and only if G is of the form A^*CA^* for some matrix C over S.

Proof. (a) If G is a $\{1,2,3\}$-inverse of A, i.e., $AGA = A$, $GAG = G$, $(AG)^* = AG$, then $G = GAG = G(AG)^* = GG^*A^*$, and so G is of the form CA^*.

Conversely, if G is a $\{1\}$-inverse of A and $G = CA^*$ for some matrix C over S, then $ACA^*A = A$. This gives $ACA^*AC^*A^* = AC^*A^*$. So $(ACA^*)(ACA^*)^* = (ACA^*)^*$. On the other hand, $(ACA^*)(ACA^*)^* = ((ACA^*)(ACA^*)^*)^* = ((ACA^*)^*)^* = ACA^*$. Thus, $(ACA^*)^* = ACA^*$, that is,

$$(AG)^* = AG.$$

This also implies

$$GAG = CA^*ACA^* = CA^*(ACA^*)^* = C(ACA^*A)^* = C(AGA)^* = CA^* = G.$$

Hence, G is a $\{1,2,3\}$-inverse of A over S.

(b) If G is a $\{1,2,4\}$-inverse of A, i.e., $AGA = A$, $GAG = G$, $(GA)^* = GA$, then $G = GAG = (GA)^*G = A^*G^*G$, and so G is of the form A^*C.

Conversely, if G is a $\{1\}$-inverse of A and $G = A^*C$ for some matrix C over S, then $AA^*CA = A$. This gives $A^*C^*AA^*CA = A^*C^*A$, that is, $(A^*CA)^*(A^*CA) = (A^*CA)^*$. On the other hand, $(A^*CA)^*(A^*CA) = ((A^*CA)^*(A^*CA))^* = A^*CA$. Thus, $(A^*CA)^* = A^*CA$, that is,

$$(GA)^* = GA.$$

It follows that

$$GAG = A^*CAA^*C = (A^*CA)^*A^*C = (AA^*CA)^*C = (AGA)^*C = A^*C = G$$

By definition, G is a $\{1,2,4\}$-inverse of A over S.

(c) If G is the MP-inverse of A, i.e., $AGA = A$, $GAG = G$, $(AG)^* = AG$, $(GA)^* = GA$, then $G = GAG = GAGAG = (GA)^*G(AG)^* = A^*G^*GG^*A^*$, and so G is of the form A^*CA^*.

Conversely, if G is a $\{1\}$-inverse of A and $G = A^*CA^*$ for some matrix C over S, then $AA^*CA^*A = A$. This gives $AA^*CA^*AC^*AA^* = AC^*AA^*$ and $A^*AC^*AA^*CA^*A = A^*AC^*A$, that is,

$$(AA^*CA^*)(AA^*CA^*)^* = (AA^*CA^*)^*,$$
$$(A^*CA^*A)^*(A^*CA^*A) = (A^*CA^*A)^*.$$

It follows that

$$(AA^*CA^*)^* = (AA^*CA^*)(AA^*CA^*)^* = ((AA^*CA^*)(AA^*CA^*)^*)^* = AA^*CA^*,$$
$$(A^*CA^*A)^* = (A^*CA^*A)^*(A^*CA^*A) = ((A^*CA^*A)^*(A^*CA^*A))^* = A^*CA^*A,$$

namely,

$$(AG)^* = AG, \qquad (GA)^* = GA.$$

Now,

$$A^*CA^*AA^*CA^* = (A^*CA^*A)^*A^*CA^* = (AA^*CA^*A)^*CA^* = A^*CA^*,$$

that is, $GAG = G$. Hence, G is the MP-inverse of A over S.

□

Corollory 4.6. *Let A be an $m \times n$ matrix over the skew polynomial ring S with an involution $a \to \overline{a}$. If $\rho(A^*A) = \rho(A)$ and A^*A is regular, then A has a $\{1,2,3\}$-inverse over S.*

Proof. Let A be as above. Since $\rho(A^*A) = \rho(A)$ and A^*A is regular, by Part (b) of Corollary 4.1, A has a $\{1\}$-inverse of the form CA^* for some matrix C over S. By Part(a) of Proposition 4.7, CA^* is a $\{1,2,3\}$-inverse of A over S. □

Theorem 4.7. *Let $A_{m\times n}$ be a matrix of rank r over the skew polynomial ring S with an involution $a \to \overline{a}$ such that A has a factorization $A = A_LA_R$ over S, where A_L is $m \times r$ and A_R is $r \times n$. Then A has a $\{1,2,3\}$-inverse over S if and only if $A_L^*A_L$ is invertible and A_R has a right inverse over S .*

Proof. Let A be as above. Then, by (1.15) and (1.18), $\rho(A_L) = r$, $\rho(A_R) = r$, and so A_L has a left inverse over $Q(S)$, A_R has a right inverse over $Q(S)$.

Suppose A has a $\{1,2,3\}$-inverse G over S. Consider A and G as matrices

over $Q(S)$. Since $AGA = A$, that is, $A_LA_RGA_LA_R = A_LA_R$, we have

$$A_RGA_L = I. \tag{4.22}$$

Thus, A_R has a right inverse over S. Also, since $(AG)^* = AG$, we have

$$G^*A_R^*A_L^* = A_LA_RG. \tag{4.23}$$

By (4.22) and (4.23),

$$A_RGG^*A_R^*A_L^*A_L = A_RGA_LA_RGA_L = I.$$

Thus, $A_L^*A_L$ has a left inverse over S. By Proposition 1.14, $A_L^*A_L$ is invertible over S.

Conversely, suppose that $A_L^*A_L$ has an inverse, denoted by $(A_L^*A_L)^{-1}$, and A_R has a right inverse, denoted by A_R^{-1}, over S. Let $G = A_R^{-1}(A_L^*A_L)^{-1}A_L^*$. Then

$$\begin{aligned} AGA =& A_LA_RGA_LA_R \\ =& A_LA_RA_R^{-1}(A_L^*A_L)^{-1}A_L^*A_LA_R \\ =& A_LA_R \\ =& A, \end{aligned}$$

$$\begin{aligned} GAG =& A_R^{-1}(A_L^*A_L)^{-1}A_L^*AA_R^{-1}(A_L^*A_L)^{-1}A_L^* \\ =& A_R^{-1}(A_L^*A_L)^{-1}A_L^*A_LA_RA_R^{-1}(A_L^*A_L)^{-1}A_L^* \\ =& A_R^{-1}(A_L^*A_L)^{-1}A_L^* \\ =& G, \end{aligned}$$

$$\begin{aligned}
(AG)^* =& (AA_R^{-1}(A_L^*A_L)^{-1}A_L^*)^* \\
=& (A_LA_RA_R^{-1}(A_L^*A_L)^{-1}A_L^*)^* \\
=& (A_L(A_L^*A_L)^{-1}A_L^*)^* \\
=& A_L((A_L^*A_L)^{-1})^*A_L^* \\
=& A_L(A_L^*A_L)^{-1}A_L^* && \text{[By (4.8)]} \\
=& A_LA_RA_R^{-1}(A_L^*A_L)^{-1}A_L^* \\
=& AA_R^{-1}(A_L^*A_L)^{-1}A_L^* \\
=& AG.
\end{aligned}$$

By definition, G is a $\{1,2,3\}$-inverse of A over S. □

4.8 Group Inverses

Let A be an $m \times m$ matrix over a ring. An $m \times m$ matrix G is called a group inverse of A, denoted by $A^{\#}$, if

$$AGA = A, \tag{4.24}$$

$$GAG = G, \tag{4.25}$$

$$AG = GA. \tag{4.26}$$

If G satisfies only (4.24) and (4.26), then G is called a commuting g-inverse of A.

The group inverse of a given matrix is unique. For if G and H are both group inverses of A, then

$$G = GAG = GAHAG = (AG)(AH)G = AHG,$$

$$H = HAH = HAGAH = H(GA)(HA) = HGA = HAG = AHG,$$

and so $G = H$. For a given matrix A, if G is a commuting g-inverse of A, then GAG is a group inverse of A. Thus, a square matrix has a group inverse if and

only if it has a commuting g-inverse.

Proposition 4.8. *Let A be a square matrix over S and $n \in \mathbb{N}$, $n \geq 2$. The following statements are equivalent.*

(i) A has a group inverse over S.

(ii) A has a $\{1\}$-inverse of the form AC for some matrix C over S.

(iii) A has a $\{1\}$-inverse of the form CA for some matrix C over S.

(iv) A has a $\{1\}$-inverse of the form ACA for some matrix C over S.

(v) $\rho(A) = \rho(A^2)$ and A^2 is regular.

(vi) $\rho(A) = \rho(A^n)$ and A^n is regular.

Further, if ACA is a $\{1\}$-inverse of A over S, then ACA is the group inverse of A.

Proof. By Corollary 4.5, (ii) to (vi) are equivalent.

$(i) \Rightarrow (ii)$. If G is a group inverse of A, then $G = GAG = AGG$. Thus, A has a $\{1\}$-inverse of the form AC for some square matrix C over S.

$(iv) \Rightarrow (i)$. Suppose A has a $\{1\}$-inverse G over S, where $G = ACA$ for some matrix C. Then

$$A = AGA = A^2CA^2 \tag{4.27}$$

By (1.18), $\rho(A) = \rho(A^2)$. Thus, there exists a matrix B over $Q(S)$ such that

$$BA^2 = A. \tag{4.28}$$

Since $A^2CA^3 = A^2$, by using (4.28), we get

$$ACA^3 = A. \tag{4.29}$$

Also, (4.27) gives $A^3CA^2 = A^2$. Using the same method as above, we get

$$A^3CA = A. \tag{4.30}$$

By (4.29) and (4.30), we have

$$GAG = ACAAACA = ACA = G, \quad AG = ACA^3ACA = ACAA = GA.$$

Therefore, G is the group inverse of A over S.

□

4.9 Drazin Inverses

Let A be an $n \times n$ matrix over the skew polynomial ring S. An $n \times n$ matrix G over S is called a Drazin inverse of A if for some positive integer k,

$$A^{k+1}G = A^k, \tag{4.31}$$

$$GAG = G, \tag{4.32}$$

$$AG = GA. \tag{4.33}$$

The Drazin inverse of a given matrix is unique. For if G and H are both Drazin inverses of A, then for some positive integer k,

$$\begin{aligned} G &= GAG = G^2A = \cdots = G^{k+1}A^k = G^{k+1}A^{k+1}H = G^{k+1}A^{k+1}HAH \\ &= G^{k+1}A^{k+2}H^2 = \cdots = G^{k+1}A^{2k+1}H^{k+1} = G^{k+1}A^kA^{k+1}H^{k+1} \\ &= GA^{k+1}H^{k+1} = A^{k+1}GH^{k+1} = A^kH^{k+1} = A^{k-1}HAHH^{k-1} \\ &= A^{k-1}H^k = \cdots = H. \end{aligned}$$

If A has a Drazin inverse G satisfying (4.31), then, by (1.18), $\rho(A^k) = \rho(A^{k+1})$. We define the smallest positive integer p such that $\rho(A^{p+1}) = \rho(A^p)$ to be the

index of A.

Proposition 4.9. *Let A, G be two matrices over the skew polynomial ring S and let p be the index of A.*

(a) If A and G satisfy (4.31), then A and G satisfy $A^{p+1}G = A^p$.

(b) If A and G satisfy $A^{p+1}G = A^p$, then A and G satisfy (4.31) for all $k \geq p$, $k \in \mathbb{N}$.

Proof. Consider A as a matrix over $Q(S)$.

(a) If A and G satisfy (4.31), then $\rho(A^k) = \rho(A^{k+1})$, and so $\rho(A^k) = \rho(A^p)$. Thus, there exists a matrix B over $Q(S)$ such that $A^p = BA^k$, which implies

$$A^p = BA^k = BA^{k+1}G = A^pAG = A^{p+1}G.$$

(b) Trivial.

□

We now establish a relation between the existence of the Drazin inverse of a given matrix A over S and the existence of a $\{1\}$-inverse of A^k for some integer k.

Theorem 4.8. *Let A be an $n \times n$ matrix over the skew polynomial ring S and let p be the index of A.*

(a) If A has a Drazin inverse over S, then A^{p+1} is regular over S.

(b) If A^{p+k} is regular over S for some integer $k \geq 1$, then both A^{p+k+1} and A^{p+k-1} are regular over S, and A has a Drazin inverse over S.

(c) If A^{2p+1} has a $\{1\}$-inverse $(A^{2p+1})^-$ over S, then $A^p(A^{2p+1})^-A^p$ is the Drazin inverse of A over S.

Proof. (a) Let G be the Drazin inverse of A over S. Then $A^{p+1} = A^pA = A^{p+1}GA$. On the other hand, $GA = G^{p+1}A^{p+1}$. Thus, $A^{p+1} = A^{p+1}G^{p+1}A^{p+1}$, and so A^{p+1} is regular over S.

(b) Let G be a $\{1\}$-inverse of A^{p+k} over S. We first show that A^{p+k+1} is regular. Since $A^{p+k}GA^{p+k} = A^{p+k}$, it follows from (1.18) that $\rho(A^{p+k}) = \rho(A^{p+k-1})$, and so there exists a matrix B over $Q(S)$, such that $A^{p+k}B = A^{p+k-1}$. Thus, we have

$$A^{p+k}GA^{p+k-1} = A^{p+k-1}. \tag{4.34}$$

Let $H = GA^{p+k-1}G$. By (4.34), we have

$$\begin{aligned} A^{p+k+1}HA^{p+k+1} &= A(A^{p+k}GA^{p+k-1})GA^{p+k+1} \\ &= AA^{p+k-1}GA^{p+k+1} \\ &= A^{p+k+1}. \end{aligned}$$

Also, by (4.34), we have $A^{p+k-1}AGA^{p+k-1} = A^{p+k-1}$. Hence, both A^{p+k+1} and A^{p+k-1} are regular over S.

The above result implies that, if A^{p+k} is regular over S for some integer $k \geq 1$, then A^{2p+1} is regular over S. Thus, to show that A has a Drazin inverse over S, it suffices to show Statement (c) of this proposition.

(c) Let $H = A^p(A^{2p+1})^-A^p$. Since $\rho(A^{2p+1}) = \rho(A^{p+1}) = \rho(A^p)$, there exist matrices B, C, D over $Q(S)$ such that

$$A^{p+1} = BA^{2p+1}, \qquad A^p = CA^{2p+1} = A^{2p+1}D.$$

It follows that

$$AH = A^{p+1}(A^{2p+1})^-A^p = BA^{2p+1}(A^{2p+1})^-A^{2p+1}D = BA^{2p+1}D = A^{p+1}D,$$

$$HA = A^p(A^{2p+1})^- A^{p+1} = CA^{2p+1}(A^{2p+1})^- AA^{2p+1}D = CA^{2p+1}AD = A^{p+1}D,$$

whence $AH = HA$. Also, we have

$$\begin{aligned}
A^{p+1}H &= A^{2p+1}(A^{2p+1})^- A^p = A^{2p+1}(A^{2p+1})^- A^{2p+1}D = A^{2p+1}D = A^p,\\
HAH &= A^p(A^{2p+1})^- A^p A^{p+1}(A^{2p+1})^- A^p\\
&= A^p(A^{2p+1})^- A^p BA^{2p+1}(A^{2p+1})^- A^{2p+1}D\\
&= A^p(A^{2p+1})^- A^p BA^{2p+1}D = A^p(A^{2p+1})^- A^p A^{p+1}D\\
&= A^p(A^{2p+1})^- A^p = H.
\end{aligned}$$

Therefore, H is the Drazin inverse of A over S.

□

The above result shows that a given matrix A of index p over S has a Drazin inverse over S if and only if A^{p+1} is regular over S. In the following theorem, we shall see that the existence of the Drazin inverse of A can also be determined by the existence of the group inverse of A^p over S.

Theorem 4.9. *Let A be a matrix of index p over the skew polynomial ring S and let $k \geq p$, $k \in \mathbb{N}$. Then A has a Drazin inverse over S if and only if A^k has a group inverse over S.*

Proof. Suppose A has a Drazin inverse G over S. We show that G^k is the group inverse of A^k over S. By (4.32), (4.33), we have $AG = A^kG^k$, $GA = G^kA^k$, $G^kA = G^{k-1}$. Hence,

$$\begin{aligned}
G^kA^kG^k &= G^kAG = G^{k-1}G = G^k,\\
G^kA^k &= GA = AG = A^kG^k.
\end{aligned}$$

Also, by Proposition 4.9, we have $A^{k+1}G = A^k$. Thus, $A^kGA = A^k$, and so

$$A^{2k}G^k = A^kG^kA^k = A^kGA = A^k.$$

By, definition, G^k is the group inverse of A^k.

Conversely, suppose A^k has a group inverse H over S. Then, by Part (v) of Proposition 4.8, A^{2k} is regular over S, and by Part (b) of Theorem 4.8, A has a Drazin inverse over S. □

After seeing the above conditions for a given matrix to have a Drazin inverse over the skew polynomial ring S, we give a result on the decomposition of a Drazin inverse of a matrix over S as follows.

Proposition 4.10. *Let A be a square matrix over the skew polynomial ring S. Then A has a Drazin inverse over S if and only if A can be uniquely expressed as $A_1 + A_2$, where*

(i) A_1 has a group inverse over S,

(ii) A_2 is nilpotent,

(iii) $A_1A_2 = A_2A_1 = 0$.

Proof. Suppose that A has a Drazin inverse G over S. Let $A_1 = AGA$ and $A_2 = A - AGA$. We first show that (i), (ii) and (iii) hold. Since $GAG = G$, $AG = GA$, we have

$$\begin{aligned} A_1GA_1 &= AGAGAGA = AGA = A_1, \\ GA_1G &= GAGAG = G, \\ A_1G &= AGAG = GAGA = GA_1, \end{aligned}$$

and so G is the group inverse of A_1 over S. Also, since $GAGA = GA$, $AG = GA$, we have

$$\begin{aligned} A_1A_2 &= AGA(A - AGA) = AGA^2 - AGAGA^2 = AGA^2 - AGA^2 = 0, \\ A_2A_1 &= (A - AGA)AGA = A^2GA - A^2GAGA = A^2GA - A^2GA = 0. \end{aligned}$$

In addition, $A^{k+1}G = A^k$ for some positive integer k, so $\rho(A^{k+1}) = \rho(A^k)$, whence we may let the index of A to be some positive integer p. By Proposition 4.9, $A^{p+1}G = A^p$, so $A^{p+1}G - A^p = 0$. Also, $AG = GA$. Thus,

$$A_2^p = (A - AGA)^p = A^p(I - AG)^p = (A^p - A^{p+1}G)(I - AG)^{p-1} = 0.$$

We now show that the decomposition $A = A_1 + A_2$ is unique. Suppose $A = B_1 + B_2$ such that B_1 has a group inverse $B_1^{\#}$ over S, B_2 is nilpotent and $B_1B_2 = B_2B_1 = 0$. Then it suffices to show $B_1 = A_1$. In the previous part we have seen that, if G is the Drazin inverse of A over S, then G is the group inverse of A_1 over S. Thus, to show $B_1 = A_1$, it suffices to show that the group inverse $B_1^{\#}$ of B_1 is the Drazin inverse of A (by the uniqueness of group inverse and that of Drazin inverse).

Since $B_1^{\#}$ is the group inverse of B_1, we have $(B_1^{\#})^2B_1 = B_1^{\#}$, and so $B_1^{\#}B_2 = (B_1^{\#})^2B_1B_2 = 0$. Similarly, we have $B_2B_1^{\#} = 0$. Thus, $AB_1^{\#} = (B_1 + B_2)B_1^{\#} = B_1B_1^{\#}$, $B_1^{\#}A = B_1^{\#}(B_1 + B_2) = B_1^{\#}B_1$, and so

$$AB_1^{\#} = B_1^{\#}A.$$

On the other hand, by assumption, $B_2^q = 0$ for some integer $q \geq 1$, $B_1B_2 = B_2B_1 = 0$, so $A^q = (B_1 + B_2)^q = B_1^q$. It follows that

$$A^{q+1}B_1^{\#} = B_1^{q-1}B_1^2B_1^{\#} = B_1^{q-1}B_1 = B_1^q = A^q,$$
$$B_1^{\#}AB_1^{\#} = A(B_1^{\#})^2 = (B_1 + B_2)(B_1^{\#})^2 = B_1(B_1^{\#})^2 = B_1^{\#}.$$

Therefore, by definition, $B_1^{\#}$ is the Drazin inverse of A, which completes the proof. □

Appendix

Maple Codes

Below are local procedures defined for finding {1}-inverses of matrices over a commutative Euclidean domain (see Algorithms 1, 2 and 3).

```
with(LinearAlgebra):
with(Student[LinearAlgebra]):
with(VectorCalculus):
with(ArrayTools):
# Packages that are used.
RowOp:=proc(B,k,i)
# Local procedure corresponding to Algorithm 1.
local rB:=2, g:=1, s:=0, t:=0, Ro:=Matrix():
rB:=RowDimension(B):
Ro:=IdentityMatrix(rB);
g:=gcdex(B[k,k],B[i,k],x,'s','t');
Ro[k,k]:=s;
Ro[k,i]:=t;
Ro[i,k]:=-B[i,k]/g;
Ro[i,i]:=B[k,k]/g;
Ro;
end proc;
```

```
ColOp:=proc(B,k,j)
# Local procedure corresponding to Algorithm 2.
local cB:=2, g:=1, s:=0, t:=0: Co:=Matrix():
cB:=ColumnDimension(B):
Co:= IdentityMatrix(cB);
g:=gcdex(B[k,k],B[k,j],x,'s','t');
Co[k,k]:=s;
Co[k,j]:=-B[k,j]/g;
Co[j,k]:=t;
Co[j,j]:=B[k,k]/g;
Co;
end proc;
```

```
GInverse:=proc(A,rA,cA)
# Local procedure corresponding to Algorithm 3.
global rA, cA:
# rA and cA are the row dimension and column dimension of the input matrix
A, respectively.
local Str:= "The input matrix has no g-inverse.":
local m:=0, n:=0, s:=min(m,n);
local k:=1, i:=1, j:=1, p:=1;
local B:=Matrix(), C:=Matrix(), MD:=Matrix(), G:= Matrix():
local E:= Matrix(), F:= Matrix():
local Ro:= Matrix(), Co:= Matrix():
local rowB:=[ ], colB:=[ ]:
local arraycol:= Array(), arrayrow:= Array():
m:=rA; n:=cA;
s:=min(m,n);
E:= IdentityMatrix(m); F:= IdentityMatrix(n);
```

```
if m=0 or n=0 then
# A is an empty matrix.
G:=Transpose(A);
return G;
elif IsZero(A) then
# A is a zero matrix.
G:=Transpose(A);
return G;
elif m=1 and n=1 then
# A is 1 × 1.
if degree(A[m,n],x)=0 then
G:=Matrix(1,1,[1/A[m,n]]);
return G;
else
return Str;
fi;
elif m=1 then
# A is 1 × n (n ≥ 2, n ∈ ℕ).
for j from 1 to n do
if not A[1,j]=0 then
p:=j;
# Find the first nonzero entry A(1, p) of A.
break;
fi;
od;
Co:=ColumnOperation(IdentityMatrix(n),[1,p]);
B:=A.Co;
F:=F.Co;
for j from 2 to n do
```

Co:=ColOp(B,1,j);

B:=B.Co;

F:=F.Co;

od;

for i to m do

for j to n do

B[i,j]:= expand(B[i,j]);

end do;

end do;

Now $A_{1\times n} = B_{1\times n}F_{n\times n}$, $B = [\gcd(A(1,1),...,A(1,n))\ 0\ \cdots\ 0]$.

if degree(B[1,1],x) > 0 then

$\gcd(A(1,1),...,A(1,n)) \neq 1$.

return Str;

else

G:=F.(Transpose(B));

return G;

fi;

elif n=1 then

A is $m \times 1$ ($m \geq 2$, $m \in \mathbb{N}$).

for i from 1 to m do

if not A[i,1]=0 then

p:=i;

Find the first nonzero entry $A(p,1)$ of A.

break;

fi;

od;

Ro:=RowOperation(IdentityMatrix(m),[1,p]);

B:=Ro.A;

E:=Ro.E;

for i from 2 to m do

Ro:=RowOp(B,1,i);

B:=Ro.B;

E:=Ro.E;

od;

for i to m do

for j to n do

B[i,j]:= expand(B[i,j]);

end do;

end do;

Now $A_{m\times 1} = E_{m\times m}B_{m\times 1}$, $B = [\gcd(A(1,1),...,A(m,1))\ 0\ \cdots\ 0]^T$.

if not B(1,1)=1 then

#$\gcd(A(1,1),...,A(m,1)) \neq 1$.

return Str;

else

G:=(Transpose(B)).E;

return G;

fi;

fi;

B:=A;

for k from 1 to s-1 do

here:

if k < s then

rowB:=[seq(B[k,j], j=k..n)];

colB:=[seq(B[i,k], i=k..m)];

if is(colB,[0 $ nops(colB)]) then

$B(k,j) = 0$ for $j = k, k+1, ..., n$.

if is(rowB,[0 $nops(rowB)]) then

$B(i,k) = 0$ for $i = k, k+1, ..., m$.

k:=k+1;

goto(here);

Go back to the step where the label “here” is.

else

for j from k+1 to n do

if not B[k,j]=0 then

p:=j;

break;

Find the first nonzero entry $B(k,p)$ in the kth row of B.

fi;

od;

Co:=ColumnOperation(IdentityMatrix(n),[k,p]);

B:=B.Co;

F:=F.Co;

fi;

else

for i from k to m do

if not B[i,k]=0 then

p:=i;

Find the first nonzero entry $B(p,k)$ in the kth column of B.

break;

fi;

od;

Ro:=RowOperation(IdentityMatrix(m),[k,p]);

B:=Ro.B;

E:=Ro.E;

fi;

for i from k+1 to m do

Ro:=RowOp(B,k,i);

```
B:=Ro.B;
E:=Ro.E;
od;
for i to m do
for j to n do
B[i,j]:= expand(B[i,j]);
end do;
end do;
C:=B;
for j from k+1 to n do
Co:=ColOp(C,k,j);
C:=C.Co;
F:=F.Co;
od;
if not C[k,k]=1 then
return Str;
else
MD:=C;
for i from k+1 to m do
Ro:=RowOp(MD,k,i);
MD:=Ro.MD;
E:=Ro.E;
od;
fi;
B:=MD;
fi:
od;
rowB:=[seq(B[m,j], j=1..n)];
colB:=[seq(B[i,n], i=1..m)];
```

```
if m > n then
if is(colB,[0$nops(colB)]) then
# B(i,n) = 0 for i = n, n+1, ..., m.
G:=F.(Transpose(B)).E;
for i to m do
for j to n do
G[j,i]:= expand(G[j,i])
end do;
end do;
return G;
else
for i from n to m do
if not B[i,n]=0 then
p:=i;
# Find the first nonzero entry B(p,n) in the nth column of B.
break;
fi;
od;
Ro:=RowOperation(IdentityMatrix(m),[n,p]);
B:=Ro.B;
E:=Ro.E;
for i from n+1 to m do
Ro:=RowOp(B,n,i);
B:=Ro.B;
E:=Ro.E;
od;
for i to m do
for j to n do
B[i,j]:= expand(B[i,j])
```

```
end do;
end do;
if not B[n,n]=1 then
return Str;
else
G:=F.(Transpose(B)).E;
for i to m do
for j to n do
G[j,i]:= expand(G[j,i])
end do;
end do;
return G;
fi;
fi;
elif n>m then
if is(rowB,[0$nops(rowB)]) then
# B(m, j) = 0 for j = m, m + 1, ..., n.
else
for j from m to n do
if not B[m,j]=0 then
p:=j;
# Find the first nonzero entry B(m, p) in the mth row of B.
break;
fi;
od;
Co:=ColumnOperation(IdentityMatrix(n),[m,p]);
B:=B.Co;
F:=F.Co;
for j from m+1 to n do
```

```
Co:=ColOp(B,m,j);
B:=B.Co;
F:=F.Co;
od:
for i to m do
for j to n do
B[i,j]:= expand(B[i,j])
end do;
end do;
if not B(m,m)=1 then
return Str;
else
G:=F.(Transpose(B)).E;
for i to m do
for j to n do
G[j,i]:= expand(G[j,i])
end do;
end do;
return G;
fi;
fi;
else
# A is m × m (m ≥ 2, m ∈ ℕ).
if not degree(B[s,s],x) > 0 then
# B(m, m) ∈ 𝔽.
if not B[s,s] =0 then
Ro:=RowOperation(IdentityMatrix(s),s,1/B[s,s]);
B:=Ro.B;
E:=Ro.E;
```

```
fi;
G:=F.(Transpose(B)).E;
for i to m do
for j to n do
G[j,i]:= expand(G[j,i])
end do;
end do;
return G;
else
return Str;
fi;
fi;
end proc;
```

Examples:

```
> restart;
> with(LinearAlgebra) :
  with(Student[LinearAlgebra]) :
  with(VectorCalculus) :
  with(ArrayTools) :
> read("RowOp.mpl") :
> read("ColOp.mpl") :
> read("GInverse.mpl") :
> A := Matrix( ); rA, cA := Dimension(A) :
```

$$A := \begin{bmatrix} \end{bmatrix} \tag{1}$$

```
> GInverse(A, rA, cA);
```

$$\begin{bmatrix} \end{bmatrix} \tag{2}$$

```
> B := Matrix(2, 3); rB, cB := Dimension(B) :
```

$$B := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{3}$$

```
> GInverse(B, rB, cB);
```

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \tag{4}$$

```
> C := Matrix(1, [5 x]); rC, cC := Dimension(C) :
```

$$C := \begin{bmatrix} 5\,x \end{bmatrix} \tag{5}$$

```
> GInverse(C, rC, cC);
```

"The input matrix has no g-inverse." (6)

```
> E := Matrix(1, 3, [1, x, x^2]); rE, cE := Dimension(E) :
```

$$E := \begin{bmatrix} 1 & x & x^2 \end{bmatrix} \tag{7}$$

```
> GInverse(E, rE, cE);
```

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \tag{8}$$

```
> F := Matrix(3, 1, [x, 2 x, x^2]); rF, cF := Dimension(F) :
```

(9)

$$F := \begin{bmatrix} x \\ 2x \\ x^2 \end{bmatrix} \tag{9}$$

```
> GInverse(F, rF, cF);
```

"The input matrix has no g-inverse." (10)

```
> G := Matrix(2, 3, [1, 2, 3, 4, 5, 6]); rG, cG := Dimension(G) :
```

$$G := \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \tag{11}$$

```
> GInverse(G, rG, cG);
```

$$\begin{bmatrix} -1 & \frac{1}{2} \\ 0 & 0 \\ \frac{2}{3} & -\frac{1}{6} \end{bmatrix} \tag{12}$$

```
> G.GInverse(G, rG, cG).G;
```

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \tag{13}$$

```
> H := Matrix(3, 2, [1, x, 0, 1, 5, 6]); rH, cH := Dimension(H) :
```

$$H := \begin{bmatrix} 1 & x \\ 0 & 1 \\ 5 & 6 \end{bmatrix} \tag{14}$$

```
> GInverse(H, rH, cH);
```

$$\begin{bmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{15}$$

```
> H.GInverse(H, rH, cH).H; # Verification
```

$$\begin{bmatrix} 1 & x \\ 0 & 1 \\ 5 & 6 \end{bmatrix} \tag{16}$$

```
> K := Matrix(2, 3, [3·x + 1, 2·x, 1, 0, x^2, x + 1]); rK, cK := Dimension(K) :
```

$$K := \begin{bmatrix} 3x+1 & 2x & 1 \\ 0 & x^2 & x+1 \end{bmatrix} \tag{17}$$

```
> GInverse(K, rK, cK);
```

$$\begin{bmatrix} 1-\frac{3}{2}x^2-\frac{3}{5}x^3 & -1-\frac{2}{5}x \\ -\frac{3}{2}+\frac{33}{10}x^2+\frac{9}{5}x^3 & \frac{11}{5}+\frac{6}{5}x \\ -\frac{9}{5}x^4-\frac{3}{2}x^3+\frac{3}{2}x^2 & -\frac{6}{5}x^2-x+1 \end{bmatrix} \quad \textbf{(18)}$$

```
> simplify(K.GInverse(K, rK, cK).K);   # Verification
```

$$\begin{bmatrix} 3x+1 & 2x & 1 \\ 0 & x^2 & x+1 \end{bmatrix} \quad \textbf{(19)}$$

```
>
```

Bibliography

[1] A. Bjerhammar, *Application of Calculus of Matrices to Method of Least Squares: With Special Reference to Geodetic Calculations*, Elander, 1951.

[2] ———, *Rectangular reciprocal matrices, with special reference to geodetic calculations*, Bulletin Géodésique (1946-1975) **20** (1951), no. 1, 188–220.

[3] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing **18** (2007), no. 4, 379–389.

[4] D. Boucher and F. Ulmer, *Coding with skew polynomial rings*, Journal of Symbolic Computation **44** (2009), no. 12, 1644–1656.

[5] M. Bronstein and M. Petkovšek, *An introduction to pseudo-linear algebra*, Theoretical Computer Science **157** (1996), no. 1, 3–33.

[6] S. L. Campbell, C. D. Meyer, and N. J. Rose, *Applications of the drazin inverse to linear systems of differential equations with singular constant coefficients*, SIAM Journal on Applied Mathematics **31** (1976), no. 3, 411–425.

[7] F. Chyzak, A. Quadrat, and D. Robertz, *Effective algorithms for parametrizing linear control systems over ore algebras*, Applicable Algebra in Engineering, Communication and Computing **16** (2005), no. 5, 319–376.

[8] P. M. Cohn, *Free Rings and Their Relations*, London Mathematical Society, 1985.

[9] ———, *Further Algebra and Applications*, Springer, 2003.

[10] ———, *Free Ideal Rings and Localization in General Rings*, vol. 3, Cambridge University Press, 2006.

[11] P. Courrieu, *Fast computation of moore-penrose inverse matrices*, Neural Information Processing Letters and Reviews (2005), 25–29.

[12] I. Fredholm, *Sur une classe déquations fonctionnelles*, Acta mathematica **27** (1903), no. 1, 365–390.

[13] M. Giesbrecht, *Factoring in skew-polynomial rings over finite fields*, Journal of Symbolic Computation **26** (1998), no. 4, 463–486.

[14] K. R. Goodearl and R. B. Warfield Jr, *An Introduction to Noncommutative Noetherian Rings*, vol. 61, Cambridge University Press, 2004.

[15] M. Hanke, *Iterative consistency: a concept for the solution of singular systems of linear equations*, SIAM Journal on Matrix Analysis and Applications **15** (1994), no. 2, 569–577.

[16] N. Jacobson, *Finite-dimensional Division Algebras over Fields*, vol. 233, Springer, 1996.

[17] V. N. Katsikis and D. Pappas, *Fast computing of the moore-penrose inverse matrix*, Electronic Journal of Linear Algebra **17** (2008), no. 1, 637–650.

[18] V. N. Katsikis, D. Pappas, and A. Petralias, *An improved method for the computation of the moore–penrose inverse matrix*, Applied Mathematics and Computation **217** (2011), no. 23, 9828–9834.

[19] S. J. Kirkland and M. Neumann, *Group inverse of m-matrices and their applications*, CRC Press, 2013.

[20] T. Y. Lam, *Lectures on Modules and Rings*, no. 189, Springer, 1999.

[21] ———, *A First Course in Noncommutative Rings*, Springer Science & Business, 2013.

[22] C. D. Meyer, Jr, *The role of the group generalized inverse in the theory of finite markov chains*, Siam Review **17** (1975), no. 3, 443–464.

[23] ———, *Analysis of finite markov chains by group inversion techniques. recent applications of generalized inverses*, Research notes in mathematics **66** (1982), 50–81.

[24] S. L. Miljkovic, *Iterative methods for computing generalized inverses of matrices*, Ph.D. thesis, University of Niš, Serbia, 2012.

[25] E. H. Moore, *On the reciprocal of the general algebraic matrix*, Bull. Amer. Math. Soc. **26** (1920), 394–395.

[26] E. Noether and W. Schmeidler, *Moduln in nichtkommutativen bereichen, insbesondere aus differential-und differenzenausdrücken*, Mathematische Zeitschrift **8** (1920), no. 1, 1–35.

[27] O. Ore, *Theory of non-commutative polynomials*, Annals of mathematics (1933), 480–508.

[28] R. Penrose, *A generalized inverse for matrices*, Mathematical proceedings of the Cambridge philosophical society, vol. 51, Cambridge University Press, 1955, pp. 406–413.

[29] R. Penrose and J. A. Todd, *On best approximate solutions of linear matrix equations*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 52, Cambridge Univ Press, 1956, pp. 17–19.

[30] K. P. S. B. Rao, *Theory of Generalized Inverses over Commutative Rings*, Taylor and Francis CRC Press, 2002.

[31] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge university press, 2013.

[32] C. Wu, *A public-key cryptosystem based on generalized inverses of matrices*, Journal of China Institute of **4** (1993), 016.

[33] C. Wu and E. Dawson, *Generalised inverses in public key cryptosystem design*, IEE Proceedings-Computers and Digital Techniques **145** (1998), no. 5, 321–326.