MATRIX ALGEBRAS:
EQUIVALENT RING RELATIONS AND SPECIAL PRESENTATIONS

by

Samuel S. Mendelson
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
In Partial fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Mathematics

Committee:

_____	Dr. Geir Agnarsson, Dissertation Director
_____	Dr. James Lawrence, Committee Member
_____	Dr. Jay Shapiro, Committee Member
_____	Dr. John B. Conway, Committee Member
_____	Dr. David Walnut, Department Chair
_____	Dr. Donna M. Fox, Associate Dean, Office of Student Affairs & Special Programs, College of Science
_____	Dr. Peggy Agouris, Dean, The College of Science
Date: _____	Spring Semester 2017 George Mason University Fairfax, VA

Matrix Algebras: Equivalent Ring Relations and Special Presentations

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

By

Samuel S. Mendelson
Master of Science
George Mason University, 2012
Bachelor of Science
George Washington University, 2008

Director: Dr. Geir Agnarsson, Associate Professor
Department of Mathematical Sciences

Spring Semester 2017
George Mason University
Fairfax, VA

Dedication

I dedicate this dissertation to my dad. For all the times he's been there, and all the times he will be.

Acknowledgments

I would like to thank my advisor Geir Agnarsson and my committee members James Lawrence, Jay Shapiro, and John Conway for their time and help. I would like to thank John Conway for all his support, advice, and motivation even after he was no longer my undergraduate advisor. I would like to thank Jay Shapiro and Neil Epstein for their help and mathematical insight. I would like to thank all the professors in the math department who helped me during my time at George Mason. I would like to thank my fellow graduate students, past and present, especially the ones who have been here with me since the beginning. I would like to thank Christine Amaya, not just for her help with all the paperwork, but for always being there to talk to. I would like to thank my mom and brother for all the love and support they have given me throughout this process. Finally, I would like to thank all my close friends who helped me through some very difficult times as I worked on my Ph.D. Without you this would have been much so much harder. Thank You.

Table of Contents

Abstract

MATRIX ALGEBRAS: EQUIVALENT RING RELATIONS AND SPECIAL PRESENTATIONS

Samuel S. Mendelson, PhD

George Mason University, 2017

Dissertation Director: Dr. Geir Agnarsson

Recognizing when a ring is a matrix ring is of significant importance in the study of algebra. A well-known result in noncommutative ring theory states that a ring R is a matrix ring if and only if it contains a set of $n \times n$ matrix units $\{e_{ij}\}_{i,j=1}^{n}$; in which case $R \cong M_2(S)$ for some S that can be completely described in terms of these matrix units. However, finding and verifying a set of matrix units can be difficult. A more recent result states that a ring R is an $(m+n) \times (m+n)$ matrix ring if, and only if, it contains three elements, a, b, and f, satisfying the two relations $af^m + f^n b = 1$ and $f^{m+n} = 0$, in which case $R \cong M_{m+n}(S)$ for some S. Under these relations very little is known about the structure of S. In this dissertation we investigate algebras over a commutative ring A (or a field k) with elements x and y that satisfy the relations $x^i y + yx^j = 1$ and $y^2 = 0$. We develop results about the structure of these algebras and their underlying rings when $\gcd(i, j) = 1$ and then generalize these results for all i and j. We then present some interesting examples demonstrating the more subtle characteristics of these algebras. Finally, we develop techniques to see when these algebras can be mapped to 2×2 matrix rings.

Chapter 1: Introduction

1.1 History and Motivation

The importance of matrix rings and algebras has been known and studied for a long time. For examples of their importance and study see [**?**] and [**?**]. However, recognizing a matrix ring or algebra is not always obvious. The following is a well-known result in noncommutative ring theory for recognizing matrix rings as stated in [**?**]. We begin with a definition.

Definition 1.1.1. *Let R be a ring and*

$$\{e_{ij} | 1 \leq i, j \leq n\} \subseteq R.$$

We say this set of elements is an $n \times n$ set of matrix units if the elements satisfy the relations

$$\sum_{i=1}^{n} e_{ii} = 1 \text{ and } e_{ij}e_{km} = \delta_{jk}e_{im},$$

where δ_{jk} is the Kronecker delta function.

If R is an $n \times n$ matrix ring, then the set of matrices with a 1 in the ij-th entry and 0 everywhere else for a set of $n \times n$ matrix units. However, the converse is true as well, (see [**?**]).

Theorem 1.1.2. *The ring $R \cong M_n(S)$ is a complete $n \times n$ matrix ring over some ring S if and only if it contains a set of $n \times n$ matrix units.*

A complete matrix ring is a matrix ring that contains every possible matrix. The complex numbers, for example, can be represented as a matrix ring that is not complete:

that is, a proper subring of a complete matrix ring that is not a complete matrix ring itself. The ring S, as defined above, can be completely determined in terms of the the set of matrix units as follows:

$$S \cong \left\{ \sum_{i=1}^{n} e_{i1} x e_{1i} | x \in R \right\}.$$

However, these matrix units can be difficult to find and tedious to verify, as shown in a set of computations in Chapter 2. In 1990, Chatters in [**?**] posed the following question: Let $\mathbb{H}$ be the integer quaternions and

$$T(n) = \begin{pmatrix} \mathbb{H} & n\mathbb{H} \\ \mathbb{H} & \mathbb{H} \end{pmatrix}.$$

For which, if any values of n is the tiled matrix ring $T(n)$ a complete matrix ring. At first glance, $T(n)$ does not appear to be a complete matrix ring. However, using properties of $\mathbb{H}$ and finding suitable matrix units, $T(n) \cong M_2(S)$ for some S (not necessarily unique) for odd values of n.

In 1990, Robson in [**?**] gave the following theorem for recognizing complete matrix rings.

Theorem 1.1.3. *The ring R is a complete $n \times n$ matrix ring $M_n(S)$ if and only if it contains elements $a_1, a_2, \ldots, a_n, f$ satisfying the relations*

$$f^n = 0 \text{ and } a_1 f^{n-1} + f a_2 f^{n-2} + \cdots + f^{n-1} a_{n-1} = 1.$$

As a consequence Robson was able to answer the question posed by Chatters in an alternative fashion. In 1996, Agnarsson, Amitsur, and Robson in [**?**] refined this result into the following two theorems, the first of which are a three-element relations.

Theorem 1.1.4. *The ring R is a complete $(m+n) \times (m+n)$ matrix ring $M_{m+n}(S)$ if and*

only if it contains elements a, b, and f satisfying the relations

$$af^m + f^n b = 1 \text{ and } f^{m+n} = 0.$$

Using this result, Agnarsson, Amitsur, and Robson investigated rings of differential operators.

In 1996, Lam and Leroy in [**?**] investigated relations for recognizing matrix rings, in particular these three-element relations. Using Theorem 1.1.4 (from [**?**]) they give an eigenring description, using a certain nilpotent element in R, for the ring S over which R is a complete $(m+n) \times (m+n)$ matrix ring. In addition, they use Theorem 1.1.4 to study Ore extension rings (or skew-polynomial rings).

Under these relations however, very little is known about the structure of the ring S. In fact, under certain circumstances, S may be the trivial ring. Their next result is of two-element relations.

Theorem 1.1.5. *The ring R is a complete $(m+n) \times (m+n)$ matrix ring $M_{m+n}(S)$ if and only if it contains elements a and f satisfying the relations*

$$a^m f^m + f^n a^n = 1 \text{ and } f^{m+n} = 0.$$

Under these two-element relations, it is easy to find matrix units and thus define the ring S. The element a as defined above can be seen as the matrix with 1's along its subdiagonal and 0's everywhere else, while the element f can be seen as the matrix with 1's along its superdiagonal and 0's everywhere else. A natural question that arises from these two-element relations: what happens if the first relation of above is replace with the relation $1 = a^i f^m + f^n a^j$? By Theorem 1.1.4, this ring will still be an $(m+n) \times (m+n)$ matrix ring; but what about the ring S? In [**?**], Agnarsson showed the following negative result.

Lemma 1.1.6. *Let the ring R contain elements a and b such that $1 = ab^m + b^n a$ and $0 = b^{m+n}$. If $m \neq n$, then R is the trivial ring.*

This result leads to the questions explored in this dissertation.

1.2 Basic Setup and Definitions

From this point on, all rings will be considered associative with a unit 1 and all homomorphisms will be unital. We begin with some definitions.

Definition 1.2.1. *(i)The* free monoid *on n indeterminates $\langle x_1, x_2, \ldots, x_n\rangle$ is the set of words made by the indeterminates x_i along with the binary operation of concatenation of words with identity, the empty word.*

(ii) The free algebra *over the ring A over n indeterminates $A\langle x_1, x_2, \ldots, x_n\rangle$ is the set of formal linear combinations over A of words made by the indeterminates x_i. Addition is defined as formal sums of elements and multiplication is defined as concatenation of basis elements extended as a bilinear operation.*

We are interested in rings with two elements, x and y, satisfying the relations $x^iy^m + y^nx^j = 1$ and $y^{m+n} = 0$. We will investigate the free object satisfying these two relations as defined below.

Definition 1.2.2. *Let $R(A; i, j, m, n) = A\langle x, y|x^iy^m+y^nx^j = 1, y^{m+n} = 0\rangle$ where $A\langle x, y|x^iy^m+y^nx^j = 1, y^{m+n} = 0\rangle$ is the free algebra over A in two indeterminates satisfying the given relations. This is equivalent to algebra $A\langle x, y\rangle/I$ where I is the two sided ideal generated by $x^iy^m + y^nx^j - 1$ and y^2.*

By Theorem 1.1.4, we have $R(A; i, j, m, n) \cong M_{m+n}(T)$ for some A-algebra T. However, we have very little information about T. Therefore, we introduce the following sets, similarly as in [**?**].

Definition 1.2.3. *Define the sets $\mathcal{A}_A, \mathcal{B}_A, \mathcal{C}_A \subseteq \mathbb{N}^4$ as follows;*

$\mathcal{C}_A$ is the set of $(i, j, m, n) \in \mathbb{N}^4$ such that $R(A; i, j, n, m)$ is non-trivial.

$\mathcal{B}_A$ is the set of $(i, j, m, n) \in \mathbb{N}^4$ such that there is a non-trivial homomorphism from

$R(A; i, j, m, n)$ *to* $M_N(A)$ *for some* $N \in \mathbb{N}$.

$\mathcal{A}_A$ *is the set of* $(i, j, m, n) \in \mathbb{N}^4$ *such that there is a non-trivial homomorphism from* $R(A; i, j, m, n)$ *to* $M_{m+n}(A)$.

The set $\mathcal{C}_A$ can be seen as the set of (i, j, m, n) such that $R(A; i, j, m, n)$ can be mapped to a set of A-linear functions $R(A; i, j, m, n) \to R(A; i, j, m, n)$ or to $\mathrm{End}_A(R(A; i, j, m, n))$; the set $\mathcal{B}_A$ can be seen as the set of (i, j, m, n) such that $R(A; i, j, m, n)$ can be mapped to a set of finite-rank matrices over A; and the set $\mathcal{A}_A$ can be seen as the set of (i, j, m, n) such that $R(A; i, j, m, n)$ can be mapped to a set "appropriately" sized matrices over A.

In [**?**], Agnarsson analyzes these sets and finds elements of each. Before beginning our analysis, we need two results, the first of which is a rephrased technical lemma from [**?**].

Lemma 1.2.4. *Let* $x \in R$, *then* x *has an* n*-th root in* $M_n(R)$ *under the natural embedding* ($r \mapsto r \cdot I$ *where* $I \in M_n(R)$ *is the identity matrix) given by*

$$\begin{pmatrix} 0 & 0 & \dots & 0 & x \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Next, we need an important result by Bergman from [**?**], namely the *Diamond Lemma*. We begin with a definition.

Definition 1.2.5. *(i) Let* $\langle X \rangle$ *be the free monoid over* n *indeterminates.* A semigroup order *is a partial order on the words of* $\langle X \rangle$ *respecting multiplication. That is if* $W_1 \leq W_2$, *then* $BW_1 \leq BW_2$ *and* $W_1C \leq W_2C$ *for* $W_1, W_2, B, C \in \langle X \rangle$.

(ii) We say $\leq$ *satisfies the* descending chain condition *if for every sequence of words in*

$\langle X \rangle$ *with*

$$W_1 \geq W_2 \geq \cdots \geq W_i \ldots,$$

there exists an N *such that* $W_i = W_N$ *for all* $i \geq N$.

There are many different semigroup orders. We will mostly use the *deglex order*, which depends on the degree and lexicographic order of each monomial. Let the indeterminates be ordered lexicographically, then the deglex order is given by $W_1 \leq W_2$ if and only if the $\deg(W_1) < \deg(W_2)$ or $\deg(W_1) = \deg(W_2)$ and W_1 comes before W_2 lexicographically. The following definitions are from [**?**].

Definition 1.2.6. *Let* $S = \{\alpha = (W_\alpha, f_\alpha)\}$ *be a family of pairs indexed by* α *where* $W_\alpha \in \langle X \rangle$ *and* $f_\alpha \in A\langle X \rangle$*, the free monoid and free* A*-algebra respectively. For each* $\alpha \in S$ *and* $B, C \in \langle X \rangle$*, let* $r_{B\alpha C} : A\langle X \rangle \to A\langle X \rangle$ *be the* A*-module homomorphism that fixes* $A\langle X \rangle$ *except for the element* $BW_\alpha C$ *which is sent to* $Bf_\alpha C$*. The set* S *is called a* reduction system *and the set* $r_{B\alpha C}$ *are called* reductions*. An element* $D \in A\langle X \rangle$ *is said to be* irreducible *if it is fixed under every* $r_{B\alpha C}$*.*

As an example corresponding to $R(A; i, j, m, n)$, let $S = \{\alpha = (y^n x^j, 1 - x^i y^m), \beta = (y^{m+n}, 0)\}$. By reduction we mean that the monomial $y^n x^j$ can be "reduced" to $1 - x^i y^m$ (or $y^n x^j = 1 - x^i y^m$) and the monomial y^{m+n} can be "reduced" to 0 (or $y^{m+n} = 0$). This however can lead to uncertainty as to how to reduce certain words. For example $y^{m+n} x^j = (y^{m+n}) x^j = y^m (y^n x^j)$.

Definition 1.2.7. *Let* S *be a reduction system with* $\alpha, \beta \in S$*. Suppose* $W_\alpha = BC$ *and* $W_\beta = CD$ *for* $B, C, D \in \langle X \rangle$*. We call this an* overlap ambiguity *as* $BCD = W_\alpha D = BW_\beta$*. We say the overlap ambiguity is* resolvable *if there exists compositions of reductions* r *and* r' *such that* $r(f_\alpha D) = r'(Bf_\beta)$*, i.e. under the two different reductions,* $W_\alpha D = BW_\beta$ *eventually reduce to the same element of* $A\langle X \rangle$*.*

Suppose that $W_\alpha = B$ *and* $W_\beta = CBD$*. We call this an* inclusion ambiguity *since* $W_\beta = CW_\alpha D$*. We say the inclusion ambiguity is* resolvable *if* f_β *and* $Cf_\alpha D$ *can be reduced*

to the same element.

We say a reduction system is complete if all ambiguities are resolvable.

The ambiguity above $y^{m+n}x^j = (y^{m+n})x^j = y^m(y^n x^j)$ is not resolvable and so our example of a reduction system is not complete. In order to resolve this ambiguity, we introduce a new reduction that would resolve this ambiguity. Since $(y^{m+n})x^j = 0x^j = 0$ and $y^m(y^n x^j) = y^m(1 - x^i y^m) = y^m - y^m x^i y^m$, we would introduce the reduction $\gamma = (y^m x^i y^m, y^m)$, or $\gamma = (y^m, y^m x^i y^m)$. We will now combine the idea of a semigroup order with that of reduction systems to determine which reduction to choose.

Definition 1.2.8. *Let $\leq$ be a semigroup order on $\langle X \rangle$ and S a reduction system. We say $\leq$ is compatible with S if f_α is a linear combination of monomials, all of which are $< W_\alpha$ for all α.*

The following is the Diamond Lemma by Bergman from [**?**], which we will use frequently.

Theorem 1.2.9. *Let A be a commutative ring, S a reduction system, $\leq$ be a semigroup order compatible with S and having the descending chain condition, and $A\langle X \rangle_{irr}$ be the set of irreducible elements under S. The following are equivalent:*

(i) All ambiguities of S are resolvable.

(i') All ambiguities of S are resolvable relative to $\leq$

(ii) All elements of $A\langle X \rangle$ are reduction unique under S.

(iii) A set of representatives of $A\langle X \rangle$ for the elements of the A-algebra $R = A\langle X \rangle / I$, determined by the generators X and the relations $W_\alpha = f_\alpha$ for all $\alpha \in S$ is given by the A-submodule $A\langle X \rangle_{irr}$ spanned by the S-irreducible monomials of $\langle X \rangle$ over A.

Under these conditions R may be identified with the free A-module $A\langle X \rangle_{irr}$, made an A-algebra by $a \cdot b = r_S(ab)$.

We will use the fact that under a complete reduction system, we may view a quotient as a free-module by taking reduction systems and making them complete. We will use the Diamond Lemma frequently to find relations in $R(A; i, j, m, n)$ and analyze $R(A; i, j, m, n)$.

In Chapter 2, we will find many structural properties of $R(A; i, j, 1, 1) = M_2(T)$ and then explicitly describe T when $\gcd(i, j) = 1$. Using this description we will generalize our results to $R(A; i, j, n, n)$ for all i and j. We will end Chapter 2 with interesting examples of $R(A; i, j, 1, 1)$ to demonstrate some of its more subtle properties for certain A, i, and j.

In Chapter 3, we will introduce a characteristic polynomial to $R(k; i, j, 1, 1)$ for k a field and a sequence generated by this polynomial. We will find necessary and sufficient conditions on this sequence so that $(i, j, 1, 1) \in \mathcal{A}_k$. Finally, we will apply these conditions to $R(k; i, j, 1, 1)$ for minimal fields.

Chapter 2: The Case of $m = n = 1$

In this chapter, we will give an explicit description of the underlying ring for the class of $R(A; i, j, m, n)$ (from Definition 1.2.2) when $\gcd(i, j) = 1$ and $m = n = 1$. For the rest of this chapter, the ring A will be commutative and we will let $m = n = 1$ unless otherwise noted.

2.1 Relations and Reductions

We begin with some technical lemmas for relations in $R(A; i, j, 1, 1)$.

Lemma 2.1.1. *For the generators $x, y \in R(A; i, j, 1, 1)$, we have the following relations:*

i) $yx^iy = yx^jy = y$

ii) $yx^{i+j}y = 0$

iii) $yx^{2i}y = -yx^{2j}y$.

Proof. We have that $x^iy + yx^j = 1$ and $y^2 = 0$. Therefore,

$y = y \cdot 1 = y(x^iy + yx^j) = yx^iy + y^2x^j = yx^iy$

Similarly, $y = (x^iy + yx^j)y = yx^jy$.

Using the above,

$$\begin{aligned} yx^jx^iy &= yx^j(x^iy + yx^j)x^iy \\ &= yx^{i+j}yx^iy + yx^jyx^{i+j}y \\ &= 2yx^{i+j}y, \end{aligned}$$

and so $yx^{i+j}y = 0$.

Finally, using these two results,

$$\begin{aligned} 0 = yx^{i+j}y &= yx^ix^jy \\ &= yx^i \cdot 1 \cdot x^jy = yx^i(x^iy + yx^j)x^jy \\ &= yx^{2i}yx^jy + x^iyx^{2j}y \\ &= yx^{2i}y + yx^{2j}y, \end{aligned}$$

and thus $yx^{2i}y = -yx^2jy$. □

Lemma 2.1.2. *The following are relations for yx^{in} and yx^{jn} respectively:*

$$yx^{in} = (-1)^n x^{jn}y + \sum_{k=0}^{n-1}(-1)^{n-1-k}x^{(n-1)j+k(i-j)} \tag{2.1}$$

$$yx^{jn} = (-1)^n x^{in}y + \sum_{k=0}^{n-1}(-1)^{k}x^{(n-1)j+k(i-j)} \tag{2.2}$$

Proof. We will proceed by induction on n. Let $n = 1$, then $yx^i = 1 - x^jy$ and $yx^j = 1 - x^iy$.

Assume (2.1) is true for n. Then

$$\begin{aligned} yx^{i(n+1)} &= \left(yx^{in}\right)x^i \\ &= (-1)^n x^{jn}yx^i + \sum_{k=0}^{n-1}(-1)^{n-1-k}x^{(n-1)j+k(i-j)+i} \end{aligned}$$

$$= (-1)^n x^{jn}(1 - x^j y) + \sum_{k=0}^{n-1} (-1)^{n-(k+1)} x^{nj+(k+1)(i-j)}$$

$$= (-1)^n x^{jn} + (-1)^{n+1} x^{j(n+1)} y + \sum_{k=1}^{n} (-1)^{n-k} x^{nj+k(i-j)}$$

$$= (-1)^{n+1} x^{j(n+1)} y + \sum_{k=0}^{n} (-1)^{n-k} x^{nj+k(i-j)}.$$

Thus,

$$yx^{in} = (-1)^n x^{jn} y + \sum_{k=0}^{n-1} (-1)^{n-1-k} x^{(n-1)j+k(i-j)}$$

for all $n \geq 1$. Similarly, assume (2.2) is true for n, then

$$yx^{j(n+1)} = \left(yx^{jn}\right) x^j$$

$$= (-1)^n x^{in} y x^j + \sum_{k=0}^{n-1} (-1)^k x^{(n-1)j+k(i-j)+j}$$

$$= (-1)^n x^{in}(1 - x^i y) + \sum_{k=0}^{n-1} (-1)^k x^{nj+k(i-j)}$$

$$= (-1)^n x^{in} + (-1)^{n+1} x^{i(n+1)} y + \sum_{k=0}^{n-1} (-1)^k x^{nj+k(i-j)}$$

$$= (-1)^{n+1} x^{j(n+1)} y + \sum_{k=0}^{n} (-1)^k x^{nj+k(i-j)}.$$

And so, by induction, we have (2.1) and (2.2) for $n \geq 1$. □

Lemma 2.1.3. *Let p and q be polynomials. If $p(x)y = q(x)y$ in $R(A; i, j, 1, 1)$, then $p(x) = q(x)$.*

Proof. Suppose $p(x)y = q(x)y$ for some polynomials p and q. Then

$$\begin{aligned} p(x)yx^j &= p(x)(1 - x^i y) \\ &= p(x) - p(x)x^i y \\ &= p(x) - x^i p(x)y, \end{aligned}$$

since $p(x)$ is a polynomial in x and thus commutes with x^i. However, $q(x)yx^j = q(x) - x^i q(x)y$ by the same argument. Since $p(x)y = q(x)y$,

$$\begin{aligned} p(x) - x^i p(x)y &= p(x)yx^j \\ &= q(x)yx^j \\ &= q(x) - x^i q(x)y \\ &= q(x) - x^i p(x)y \end{aligned}$$

and thus $p(x) = q(x)$. □

These lemmas will make proving the following theorems a little more manageable.

Theorem 2.1.4. $R(k; i, j, 1, 1) = R(k; j, i, 1, 1)$

Proof. We know $x^i y + yx^j = 1$ and $y^2 = 0$ and, using Lemma 2.1.1, we have

$$\begin{aligned} x^j y + yx^i &= (x^i y + yx^j)(x^j y + yx^i) \\ &= x^i(yx^j y) + x^i y^2 x^j + yx^{2j} y + yx^j yx^i \\ &= x^i y + yx^{2j} y + yx^i, \end{aligned}$$

and so $yx^{2j}y = x^jy - x^iy$. Similarly, expanding $(x^jy+yx^i)(x^iy+yx^j)$, we get $yx^{2i}y = yx^i - yx^j$. By Lemma 2.1.1 again, we know that $yx^{2i}y = -yx^{2j}y$, so $x^jy + yx^i = x^iy + yx^j = 1$, thus $R(A;i,j,1,1) \subseteq R(A;j,i,1,1)$. By symmetry, we see $x^jy + yx^i = 1$ and $y^2 = 0$ implies $x^iy + yx^j = 1$ in $R(A;j,i,1,1)$, and so $x^iy + yx^j = 1$ in $R(A;j,i,1,1) \subseteq R(A;i,j,1,1)$. Thus, $R(A;i,j,1,1) = R(A;j,i,1,1)$. □

This result is stronger than it first appears. It is clear that $R(A;i,j,1,1)$ is anti-isomorphic to $R(A;j,i,1,1)$. However, the above result shows that they are not just isomorphic, but actually equal. Without loss of generality, we will now assume $i \geq j$.

Lemma 2.1.5. *If $i \neq j$, then x is invertible in $R(A;i,j,1,1)$.*

Proof. By Theorem 2.1.4, we may assume $i > j$ without loss of generality. Then,

$$\begin{aligned} 1 &= x^iy + yx^j \\ &= x^{i-j}(x^jy) + yx^j \\ &= x^{i-j}(1 - yx^i) + yx^j \\ &= (x^{i-j-1} - x^{i-j}yx^{i-1} + yx^{j-1})x \end{aligned}$$

Similarly, we can show $1 = x(x^{j-1}y + x^{i-j-1} - x^{i-1}yx^{i-j})$, and so x is invertible. □

We are now able to show an important relation for x.

Theorem 2.1.6. *Let $i \geq j$ and $\gcd(i,j) = d$, then in $R(A;i,j,1,1)$ we have*

$$x^{((i+j)/d-1)(i-j)} = \sum_{k=1}^{(i+j)/d-1} (-1)^{k+1} x^{((i+j)/d-1-k)(i-j)}.$$

Proof. We will evaluate the element $yx^{(ij)/d}y$ two ways using our relation results for yx^{in}

and yx^{jn}. Let $a = i/d$ and $b = j/d$. By Lemma 2.1.2 we have

$$yx^{(ij)/d}y = \sum_{k=0}^{b-1}(-1)^{b-1-k}x^{(b-1)j+k(i-j)}y \text{ and } yx^{(ij)/d}y = \sum_{k=0}^{a-1}(-1)^{k}x^{(a-1)j+k(i-j)}y$$

for $n = b$ and $n = a$ respectively. And so,

$$\sum_{k=0}^{a-1}(-1)^{k}x^{(a-1)j+k(i-j)}y = \sum_{k=0}^{b-1}(-1)^{b-1-k}x^{(b-1)j+k(i-j)}y.$$

Using Lemma 2.1.3

$$0 = \sum_{k=0}^{b-1}(-1)^{b-k}x^{(b-1)j+k(i-j)} + \sum_{k=0}^{a-1}(-1)^{k}x^{(a-1)j+k(i-j)}.$$

Since $aj = bi$ we have, $(b-1)j + k(i-j) = (a-1)j + (k-b)(i-j)$, and so

$$\sum_{k=0}^{a-1}(-1)^{k}x^{(a-1)j+k(i-j)} = \sum_{k=b}^{a+b-1}(-1)^{b-k}x^{(b-1)j+k(i-j)}.$$

Hence,

$$0 = \sum_{k=0}^{b-1}(-1)^{b-k}x^{(b-1)j+k(i-j)} + \sum_{k=b}^{a+b-1}(-1)^{b-k}x^{(b-1)j+k(i-j)} = \sum_{k=0}^{a+b-1}(-1)^{b-k}x^{(b-1)j+k(i-j)}.$$

Since x is invertible by Theorem 2.1.5, we obtain

$$0 = \sum_{k=0}^{a+b-1}(-1)^{b-k}x^{k(i-j)},$$

and by reindexing and shifting the last term we have,

$$x^{(a+b-1)(i-j)} = \sum_{k=1}^{a+b-1} (-1)^{k+1} x^{(a+b-1-k)(i-j)}.$$

□

Writing out the above sum, we see that the relation in Theorem 2.1.6 gives an alternating series relation for $x^{(i+j)/d-1)(i-j)}$. Letting $m = (i+j)/d$ we have

$$x^{(m-1)(i-j)} = x^{(m-2)(i-j)} - x^{(m-3)(i-j)} + \cdots + (-1)^{(i+j)/d}.$$

Corollary 2.1.7. *If $d = \gcd(i, j)$, then $x^{(i^2-j^2)/d} = (-1)^{(i+j)/d}$.*

Proof. By Theorem 2.1.6, we have $x^{((i+j)/d-1)(i-j)} = \sum_{k=1}^{(i+j)/d-1} (-1)^{k+1} x^{((i+j)/d-1-k)(i-j)}$. Multiplying both sides of this relation by x^{i-j} and using Theorem 2.1.6 again, we get

$$\begin{aligned}
x^{(i+j)(i-j)/d} &= \sum_{k=1}^{(i+j)/d-1} (-1)^{k+1} x^{((i+j)/d-k)(i-j)} \\
&= x^{((i+j)/d-1)(i-j)} + \sum_{k=2}^{(i+j)/d-1} (-1)^{k+1} x^{((i+j)/d-k)(i-j)} \\
&= \sum_{k=1}^{(i+j)/d-1} (-1)^{k+1} x^{((i+j)/d-k-1)(i-j)} - \sum_{k=1}^{(i+j)/d-2} (-1)^{k+1} x^{((i+j)/d-k-1)(i-j)} \\
&= (-1)^{(i+j)/d},
\end{aligned}$$

proving our claim. □

If $i \neq j$, Corollary 2.1.7 shows that x is a root of unity.

Theorem 2.1.8. *The elements x^{i+j} and $x^i - x^j$ are in the center of $R(A; i, j, 1, 1)$.*

Proof. We know that powers of x commute and thus $(x^{i+j})x = x(x^{i+j})$ and $(x^i - x^j)x = x(x^i - x^j)$. It remains to show that these two elements commute with y. So

$$\begin{aligned} y(x^{i+j}) &= (yx^i)x^j \\ &= (1 - x^j y)x^j \\ &= x^j - x^j y x^j \\ &= x^j - x^j(1 - x^i y) \\ &= (x^{i+j})y, \end{aligned}$$

$$\begin{aligned} y(x^i - x^j) &= yx^i - yx^j \\ &= (1 - x^j y) - (1 - x^i y) \\ &= (x^i - x^j)y. \end{aligned}$$

Therefore, since both elements commute with both x and y, they commute with everything in $R(A; i, j, 1, 1)$. □

Theorem 2.1.9. *Let $\gcd(i, j) = d$. There exists polynomials $p, q \in A[x]$ both with coefficients alternating between 1 and -1, such that $yx^d = p(x) + q(x)y$ in $R(A; i, j, 1, 1)$.*

Proof. Suppose $i = j$. Then $\gcd(i, j) = i$ and $yx^i = 1 - x^i y$.

Now suppose $i \neq j$ and let $d = \gcd(i, j)$. Since $d = \gcd(i + j, j)$, there exist $m, n \in \mathbb{N}$ such that $d = nj - m(i + j)$, and so $yx^{nj} = yx^{m(i+j)+d}$. By Theorem 2.1.8, x^{i+j} is in the

center of $R(A;i,j,1,1)$ and so by Lemma 2.1.2 we obtain

$$x^{m(i+j)}yx^d = yx^{m(i+j)+d} = yx^{nj} = (-1)^n x^{in}y + \sum_{k=0}^{n-1}(-1)^k x^{(n-1)j+k(i-j)}. \tag{2.3}$$

Now, by Corollary 2.1.5, the inverse of x is a power of x and hence $x^r x^{m(i+j)} = 1$ for some r. Therefore, by (2.3) we have

$$yx^d = (-1)^n x^{in+r}y + \sum_{k=0}^{n-1}(-1)^k x^{(n-1)j+k(i-j)+r}.$$

□

Corollary 2.1.10. *If* $\gcd(i,j) = 1$*, then* $R(A;i,j,1,1)$ *is a finitely-generated module over* A *with a generating set of cardinality at most* $2(i+j-1)(i-j)$*.*

Proof. Since $\gcd(i,j) = 1$, by Theorems 2.1.6 and 2.1.9, we have relations which work as reductions for x^n and yx respectively, where $n \geq (i+j-1)(i-j)$. Using these reductions, we can write every monomial/word of x and y in $R(A;i,j,1,1)$ as an A-linear combination of elements from $\{1, x, x^2, \ldots, x^{(i+j-1)(i-j)-1}, y, xy, \ldots, x^{(i+j-1)(i-j)-1}y\}$. Hence, $R(A;i,j,1,1)$ is a finitely-generated A-module with generating set of cardinality at most $2(i+j-1)(i-j)$. □

2.2 Matrix Descriptions

In what follows, we will obtain a complete description of the A-algebra $R(A;i,j,1,1)$ when $\gcd(i,j) = 1$. By Theorem 1.3 of [**?**], letting $n = 2$, $a = x^i$, $b = x^j$, and $f = y$, then $\{E_{hk} | 1 \leq h,k \leq 2\}$, where $E_{hk} = y^{h-1}x^i yx^{j(k-1)}$ form a set of 2×2 matrix units, and hence we have the following theorem.

Theorem 2.2.1. *There exists an* A*-algebra* L *such that* $R(A;i,j,1,1) \cong M_2(L)$*.*

If we let $e_{hk} = E_{(3-h)(3-k)}$ for each h and k, then $\{e_{hk} | 1 \leq h, k \leq 2\}$ also forms a complete set of 2×2 matrix units where $e_{11} = yx^j$, $e_{12} = y$, $e_{21} = x^i yx^j$, and $e_{22} = x^i y$. We can verify the matrix-unit relations directly as follows:

$$e_{11}e_{11} = yx^j yx^j = yx^j = e_{11}$$

$$e_{11}e_{12} = yx^j y = y = e_{12}$$

$$e_{11}e_{21} = yx^j x^i yx^j = 0$$

$$e_{11}e_{22} = yx^i x^j y = 0$$

$$e_{12}e_{11} = yyx^j = 0$$

$$e_{12}e_{12} = yy = 0$$

$$e_{12}e_{21} = yx^i yx^j = yx^j = e_{11}$$

$$e_{12}e_{22} = yx^i y = y = e_{12}$$

$$e_{21}e_{11} = x^i yx^j yx^j = x^i yx^j = e_{21}$$

$$e_{21}e_{12} = x^i yx^j y = x^i y = e_{22}$$

$$e_{21}e_{21} = x^i yx^j x^i yx^j = 0$$

$$e_{21}e_{22} = x^i yx^j x^i y = 0$$

$$e_{22}e_{11} = x^i yyx^j = 0$$

$$e_{22}e_{12} = x^i yy = 0$$

$$e_{22}e_{21} = x^i yx^i yx^j = x^i yx^j = e_{21}$$

$$e_{22}e_{22} = x^i yx^i y = x^i y = e_{22}$$

$$e_{11} + e_{22} = yx^j + x^i y = 1.$$

Using the Theorem 2.2.1 and the 2×2 matrix units $\{e_{hk} | 1 \leq h, k \leq 2\}$, we will now view $R(A; i, j, 1, 1)$ as the matrix ring $M_2(L)$.

By Theorem 2.2.1 and the 2×2 matrix units $\{e_{hk} | 1 \leq h, k \leq 2\}$, we have an isomorphism $\phi : R(A; i, j, 1, 1) \to M_2(L)$. Identifying $R(A; i, j, 1, 1)$ with $M_2(L)$ via ϕ, we have

$$yx^j = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, x^i yx^j = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \text{ and } x^i y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

since $yx^j = e_{11}$, $y = e_{12}$, $x^i yx^j = e_{21}$, and $x^i y = e_{22}$. Letting

$$x^j = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } x^i = \begin{pmatrix} p & q \\ s & t \end{pmatrix}$$

we get the equations

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} p & q \\ s & t \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence, $d = p = 0$ and $c = s = 1$. Since $x^j x^i = x^i x^j$, we obtain

$$\begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & q \\ 1 & t \end{pmatrix} = \begin{pmatrix} 0 & q \\ 1 & t \end{pmatrix} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}$$

and hence $q = b$, $t = -a$, $aq = -bt$, and so $ab = ba$. Further,

$$x^{i+j} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \text{ and } x^j - x^i = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

And so, by Theorem 2.1.8, a and b are in the center of L.

Claim 2.2.2. *If a and b are as above, then a and b commute and are in the center of L. And thus $A[a, b] \subseteq L$.*

If $i \neq j$, since x is invertible by Theorem 2.1.5, so is x^{i+j} and hence, so is b. Now suppose $\gcd(i, j) = 1$. If $i > j$, then there exist $\alpha, \beta \in \mathbb{N}_0$ such that $1 = \alpha j - \beta i$ and so

$$x = x^{\alpha j - \beta i} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{\alpha} \begin{pmatrix} 0 & b \\ 1 & -a \end{pmatrix}^{-\beta} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{\alpha} \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{\beta} \frac{1}{b^{\beta}} \in M_2(A[a, b]).$$

Now, if $i = j$, then $i = j = 1$ and so

$$x = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 1 & -a \end{pmatrix}$$

and so $a = 0$ and

$$x = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \in M_2(A[a, b]).$$

Therefore, if $\gcd(i, j) = 1$, then there is an isopmorphism from $R(A; i, j, 1, 1)$ to $M_2(A[a, b])$. And thus $L \subseteq A[a, b]$ and therefore $L = A[a, b]$. This is summed up in the following proposition.

Proposition 2.2.3. *If a and b are as in Claim 2.2.2 and $\gcd(i, j) = 1$, then $R(A; i, j, 1, 1) \cong$*

$M_2(A[a,b])$ *as* A*-algebras. In particular,* L *is commutative.*

We will focus our attention on the case when $\gcd(i,j) = 1$. Under this assumption, by Theorem 2.1.9, we get a commuting rule for yx in $R(A; i, j, 1, 1)$. We begin with a definition.

Definition 2.2.4. *Let* $A[s,t]$ *be the polynomial ring in two variables* s *and* t *over* A *and let* $f : \mathbb{N}_0 \to A[s,t]$ *be defined recursively in the following way:* $f(0) = 0$, $f(1) = 1$, *and* $f(n) = tf(n-1) + sf(n-2)$ *for* $n \geq 2$.

This function will serve an important role, as evidenced by the following lemma.

Lemma 2.2.5. *For* $n \geq 1$, *we have*

$$\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f(n+1) & sf(n) \\ f(n) & sf(n-1) \end{pmatrix}.$$

Proof. We will induct on n. A base case of $n = 1$ is clear since $f(0) = 0$, $f(1) = 1$ and $f(2) = tf(1) + sf(0) = t$. Now assume

$$\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f(n+1) & sf(n) \\ f(n) & sf(n-1) \end{pmatrix}.$$

Then,

$$\begin{aligned} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{n+1} &= \begin{pmatrix} f(n+1) & sf(n) \\ f(n) & sf(n-1) \end{pmatrix} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} tf(n+1) + sf(n) & sf(n+1) \\ tf(n) + sf(n-1) & sf(n) \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} f(n+2) & sf(n+1) \\ f(n+1) & sf(n) \end{pmatrix}.$$

Thus, by induction,

$$\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f(n+1) & sf(n) \\ f(n) & sf(n-1) \end{pmatrix}.$$

□

Note the following observation:

Observation. *If $M_n(A) \cong M_n(B)$ for commutative rings (algebras) A and B where $n \geq 1$, then $A \cong B$ as rings (algebras).*

Proof. Looking at the centers of $M_n(A)$ and $M_n(B)$, we obtain

$$A \cong Z\left((M_2(A)\right) \cong Z\left(M_2(B)\right) \cong B.$$

□

By papers [**?**] and [**?**], the condition that A and B are commutative is necessary; in fact, as shown in [**?**] there is an uncountable family of pairwise non-isomorphic rings $\{S_\alpha\}$ such that $M_2(S_\alpha) \cong M_2(S_\beta)$. In fact all S_α are Noetherian domains that are finitely-generated over their centers.

Theorem 2.2.6. *Let f be defined as above. If $\gcd(i,j) = 1$, then $R(A; i, j, 1, 1) \cong M_2(A[s,t]/I)$ where*

$$I = \left(f(i+j), f(i+j-1) - s^{j-1}, s^{i-j} - (-1)^{i-j}\right)$$

where $A[s,t]$ is the polynomial ring in two variables, s and t, over A.

Before beginning our proof, we discuss some interesting consequences of Theorem 2.2.6.

First, for any ring R, the matrix ring $M_n(R)$ and R are *Morita equivalent* (see [**?**]), meaning there is an *equivalence* of their modules in a category theory sense. Therefore, by Theorem 2.2.6, we have that $R(A; i, j, 1, 1)$ is Morita equivalent to a commutative ring when $\gcd(i, j) = 1$.

For the next consequence, we begin with a definition.

Definition 2.2.7. *A* polynomial identity ring (or PI ring) R *is a ring such that there exists a "polynomial" (with non-commuting indeterminates)* $p(x_1, x_2, \ldots, x_n) \in R\langle x_1, x_2, \ldots, x^n\rangle$ *such that* $p(r_1, r_2, \ldots, r_n) = 0$ *for all* $r_i \in R$.

For example, a commutative ring R is a PI ring since it satisfies the identity $xy - yx = 0$. Similarly, 2×2 matrix rings are also PI rings, satisfying the *Hall identity*

$$(xy - yx)^2 z = z(xy - yx)^2,$$

or more generally the Amitsur-Levitzki identity

$$S_{2n}(x_1, x_2, \ldots, x_{2n}) = \sum_{\pi \in \mathrm{Sym}(2n)} (\mathrm{sgn}(\pi)) x_{\pi 1} x_{\pi 2} \ldots x_{\pi 2n} = 0$$

where $n = 2$. (see [**?**]). Therefore, Theorem 2.2.6 gives that $R(A; i, j, 1, 1)$ is a polynomial identity ring when $\gcd(i, j) = 1$.

Proof. (Theorem 2.2.6) Case 1: Suppose $i = j$. Then $i, j = 1$, and

$$x = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ 1 & -a \end{pmatrix}.$$

Then $a = 0$ and $L = A[b]$. Now, $f(i + j) = f(2) = t$, $f(i + j - 1) = f(1) = 1$, and $s^{i-j} = 1 = (-1)^{i-j}$. Then $A[s, t]/I \cong A[s]$. Thus, $R(A; i, j, 1, 1) \cong M_2(A[s, t]/I)$.

Case 2: Suppose $i \neq j$. Let $I = (f(i+j-1) - s^{j-1}, f(i+j), s^{i-j} - (-1)^{i-j})$. One thing to note is that s^{-1} exists in $A[s,t]/I$ and is given by $s^{-1} = (-1)^{i-j}s^{i-j-1}$. Now, since $\gcd(i,j) = 1$, there exist $\alpha, \beta \in \mathbb{N}_0$ such that $\alpha j - \beta i = 1$. Let $X \in M_2(A[s,t]/I)$ be given by

$$X = \frac{1}{s^b}\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{\alpha+\beta} \quad \text{and } Y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ where } \frac{1}{s^b} = \begin{pmatrix} s^{-b} & 0 \\ 0 & s^{-b} \end{pmatrix}.$$

We now obtain by direct matrix computation that

$$\begin{aligned}
X^j &= \frac{1}{s^{bj}}\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{aj+bj} \\
&= \frac{1}{s^{bj}}\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{1+bi+bj} \\
&= \frac{1}{s^{bj}}\left(\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{i+j}\right)^b \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix} \\
&= \frac{1}{s^{bj}}\begin{pmatrix} f(i+j+1) & sf(i+j) \\ f(i+j) & sf(i+j-1) \end{pmatrix}^b \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix} \\
&= \frac{1}{s^{bj}}\begin{pmatrix} tf(i+j)+sf(i+j-1) & 0 \\ 0 & s^j \end{pmatrix}^b \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix} \\
&= \frac{1}{s^{bj}}\begin{pmatrix} s^{bj} & 0 \\ 0 & s^{bj} \end{pmatrix}\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix},$$

and

$$\begin{aligned}
X^i &= \frac{1}{s^{bi}} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{ai+bi} \\
&= \frac{1}{s^{bi}} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{ai+aj-1} \\
&= \frac{1}{s^{bi}} \left(\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{i+j} \right)^{a} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} \\
&= \frac{1}{s^{bi}} \begin{pmatrix} f(i+j+1) & sf(i+j) \\ f(i+j) & sf(i+j-1) \end{pmatrix}^{a} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} \\
&= \frac{1}{s^{bi}} \begin{pmatrix} s^j & 0 \\ 0 & tf(i+j) + sf(i+j-1) \end{pmatrix}^{a} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} \\
&= \frac{1}{s^{bi}} \begin{pmatrix} s^{aj} & 0 \\ 0 & s^{aj} \end{pmatrix} \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} \\
&= s \begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 0 & s \\ 1 & -t \end{pmatrix},
\end{aligned}$$

since

$$\begin{pmatrix} t & s \\ 1 & 0 \end{pmatrix}^{-1} = \frac{1}{s}\begin{pmatrix} 0 & s \\ 1 & -t \end{pmatrix}.$$

Thus $X^iY + YX^j = I$ and $Y^2 = 0$ in $M_2(A[s,t]/I)$, so there is a homomorphism from $R(A;i,j,1,1)$ to $M_2(A[s,t]/I)$ where $x \mapsto X$ and $y \mapsto Y$ is well-defined. Further

$$x^{i+j} \mapsto \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} \text{ and } x^j - x^i \mapsto \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}.$$

Thus the homomorphism is a surjection. This homomorphism induces a surjection from L to $A[s,t]/I$ satisfying $b \mapsto s$ and $a \mapsto t$ since L is commutative.

Now, in L, since

$$(x^j)^{i+j} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}^{i+j} = \begin{pmatrix} f(i+j+1) & bf(i+j) \\ f(i+j) & bf(i+j-1) \end{pmatrix}$$

by Lemma 2.2.5 and

$$(x^j)^{i+j} = (x^{i+j})^j = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}^j = \begin{pmatrix} b^j & 0 \\ 0 & b^j \end{pmatrix}.$$

Thus, since b is invertible, $f(i+j-1) = b^{j-1}$ and $f(i+j) = 0$. Therefore, a and b satisfy the same relations as t and s in I respectively. So $L \subseteq A[s,t]/I$ and therefore $L \cong A[s,t]/I$ and so $R(A;i,j,1,1) \cong M_2(A[s,t]/I)$. □

In [**?**], it is shown that for $A = k$ a field, then $R(k;i,j,1,1)$ always maps to some $M_N(k)$

and is therefore non-zero. By using different methods, we have shown $R(A; i, j, 1, 1)$ is isomorphic to a 2×2 matrix ring over a commutative ring for any commutative ring A if $\gcd(i, j) = 1$.

It remains to show that if $\gcd(i, j) = 1$, then $R(A; i, j, 1, 1) \neq \{0\}$. For that, we need a few technical results for the function f. The following lemma can be shown with simple induction arguments.

Lemma 2.2.8. *As a polynomial of t:*

(a) $f(n)$ is monic with degree $n - 1$.

(b) $f(2n)$ has no constant term.

(c) $f(2n + 1)$ has constant term s^n.

Lemma 2.2.9. *Let $A[s, t] \to A[t]$ by $s \mapsto -1$ and let $\bar{f}$ be the image of f under this map. So, $\bar{f}(n) = t\bar{f}(n - 1) - \bar{f}(n - 2)$. In this case, for each $n \geq 1$, we have:*

$$\bar{f}(2n - 1) = (\bar{f}(n) + \bar{f}(n - 1))(\bar{f}(n) - \bar{f}(n - 1)), \tag{2.4}$$

$$\bar{f}(2n) - 1 = (\bar{f}(n + 1) - \bar{f}(n))(\bar{f}(n) + \bar{f}(n - 1)), \tag{2.5}$$

$$\bar{f}(2n) + 1 = (\bar{f}(n + 1) + \bar{f}(n))(\bar{f}(n) - \bar{f}(n - 1)). \tag{2.6}$$

Proof. To prove (2.4), we will use induction on n. When $n = 1$, $\bar{f}(1) = 1 = (\bar{f}(1) + \bar{f}(0))(\bar{f}(1) - \bar{f}(0))$. Suppose now

$$\bar{f}(2m - 1) = (\bar{f}(m) + \bar{f}(m - 1))(\bar{f}(m) - \bar{f}(m - 1)) = \bar{f}(m)^2 - \bar{f}(m - 1)^2$$

for all $m \leq n$. Then, by the defining recursion, we get

$$\begin{aligned} \bar{f}(2n + 1) &= t\bar{f}(2n) - \bar{f}(2n - 1) \\ &= t[t\bar{f}(2n - 1) - \bar{f}(2n - 2)] - \bar{f}(2n - 1) \end{aligned}$$

$$= t^2\bar{f}(2n-1) - t\bar{f}(2n-2) - \bar{f}(2n-1)$$

$$= t^2\bar{f}(2n-1) - [\bar{f}(2n-1) + \bar{f}(2n-3)] - \bar{f}(2n-1)$$

$$= (t^2-2)\bar{f}(2n-1) - \bar{f}(2n-3).$$

Using the induction hypothesis and defining recursion, we further get

$$\begin{aligned}
\bar{f}(2n+1) &= (t^2-2)[\bar{f}(n)^2 - \bar{f}(n-1)^2] - [\bar{f}(n-1)^2 - \bar{f}(n-2)^2] \\
&= (t^2-2)[(t\bar{f}(n-1) - \bar{f}(n-2))^2 - \bar{f}(n-1)^2] - [\bar{f}(n-1)^2 - \bar{f}(n-2)^2] \\
&= (t^4 - 3t^2 + 1)\bar{f}(n-1)^2 - (2t^3 - 4t)\bar{f}(n-1)\bar{f}(n-2) + \\
&\quad (t^2-1)\bar{f}(n-2)^2.
\end{aligned}$$

Again, using the defining recurrence for $\bar{f}(n+1)$ and $\bar{f}(n)$, we obtain

$$\begin{aligned}
\bar{f}(n+1)^2 - \bar{f}(n)^2 &= (\bar{f}(n+1) + \bar{f}(n))(\bar{f}(n+1) - \bar{f}(n)) \\
&= \big([t\bar{f}(n) - \bar{f}(n-1)] + \bar{f}(n)\big)\big([t\bar{f}(n) - \bar{f}(n-1)] - \bar{f}(n)\big) \\
&= ((t+1)\bar{f}(n) - \bar{f}(n-1))((t-1)\bar{f}(n) - \bar{f}(n-1)) \\
&= ((t+1)[t\bar{f}(n-1) - \bar{f}(n-2)] - \bar{f}(n-1))\cdot \\
&\quad ((t-1)[t\bar{f}(n-1) - \bar{f}(n-2)] - \bar{f}(n-1)) \\
&= ((t^2+t-1)\bar{f}(n-1) - (t+1)\bar{f}(n-2))\cdot \\
&\quad ((t^2-t-1)\bar{f}(n-1) - (t-1)\bar{f}(n-2)) \\
&= (t^4 - 3t^2 + 1)\bar{f}(n-1)^2 - (2t^3 - 4t)\bar{f}(n-1)\bar{f}(n-2) +
\end{aligned}$$

$$(t^2-1)\bar{f}(n-2)^2.$$

Hence, we obtain from the last two displayed relations

$$\bar{f}(2n+1) = (\bar{f}(n+1)+\bar{f}(n-1))(\bar{f}(n+1)-\bar{f}(n)).$$

And thus (2.4) is proven by induction.

We will use induction to prove both (2.5) and (2.6) simultaneously. When $n = 1$,

$$\bar{f}(2)-1 = t-1 = (\bar{f}(2)-\bar{f}(1))(\bar{f}(1)+\bar{f}(0))-1$$

and

$$\bar{f}(2)+1 = t+1 = (\bar{f}(2)+\bar{f}(1))(\bar{f}(1)-\bar{f}(0))+1.$$

Suppose

$$\bar{f}(2m)-1 = (\bar{f}(m+1)-\bar{f}(m))(\bar{f}(m)+\bar{f}(m-1))$$

and

$$\bar{f}(2m)+1 = (\bar{f}(m+1)+\bar{f}(m))(\bar{f}(m)-\bar{f}(m-1))$$

for all $m \leq n$. Using the defining recurrence, (2.4), and our induction hypothesis we get,

$$\begin{aligned}
\bar{f}(2n+2) &= t\bar{f}(2n+1)-\bar{f}(2n) \\
&= t(\bar{f}(n+1)-\bar{f}(n))(\bar{f}(n+1)+\bar{f}(n)) - \left[(\bar{f}(n+1)-\bar{f}(n))(\bar{f}(n)+\bar{f}(n-1))+1\right] \\
&= (\bar{f}(n+1)-\bar{f}(n))(t\bar{f}(n+1)+t\bar{f}(n)-\bar{f}(n)-\bar{f}(n-1))-1 \\
&= (\bar{f}(n+1)-\bar{f}(n))(\bar{f}(n+2)+\bar{f}(n+1))-1.
\end{aligned}$$

Thus $\bar{f}(2n+2)+1 = (\bar{f}(n+1)-\bar{f}(n))(\bar{f}(n+2)+\bar{f}(n+1))$. Similarly, $\bar{f}(2n+2)-1 = (\bar{f}(n+1)+\bar{f}(n))(\bar{f}(n+2)-\bar{f}(n+1))$, which completes our proof.

□

We will now argue directly that if $\gcd(i,j) = 1$, then $R(A; i, j, 1, 1) \neq \{0\}$.

Theorem 2.2.10. *As defined above, if* $\gcd(i,j) = 1$*, then* $I \neq A[s,t]$ *and thus* $R \neq \{0\}$*.*

Proof. Case 1: Suppose $i + j$ is even. Let $A[s,t] \to A[t]$ be the evaluation such that $s \mapsto 1$. Then $\bar{I} = (\bar{f}(i+j-1) - 1, \bar{f}(i+j), 0)$. By Lemma 2.2.8, we have that $\bar{f}(i+j-1)$ has constant term 1 and so both $\bar{f}(i+j-1) - 1$ and $\bar{f}(i+j)$ have no constant term. So $I \subseteq (t)$ and thus $\bar{I} \neq A[t]$ and $I \neq A[s,t]$. Therefore, $R \neq \{0\}$.

Case 2: Suppose $i+j$ is odd. Let $A[s,t] \to A[t]$ be the evaluation such that $s \mapsto -1$. Then $\bar{I} = (\bar{f}(i+j-1) - (-1)^{j-1}, \bar{f}(i+j), 0)$. Regardless of the parity of $j-1$, $\bar{f}(i+j-1) - (-1)^{j-1}$ and $\bar{f}(i+j)$ are monic, by Lemma 2.2.8, and share a common factor by the Lemma 2.2.9, and thus $\bar{I} \neq A[t]$ and so $I \neq k[s,t]$. Therefore, $R \neq \{0\}$. □

The following are corollaries of the above theorem.

Corollary 2.2.11. *If* $\gcd(i,j) = 1$ *and* $A[s,t]$ *has an evaluation* $\psi : A[s,t] \to A$ *such that* $(\psi \circ f)(i+j) = 0$*,* $(\psi \circ f)(i+j-1) = \phi(s^{j-1})$*, and* $(\psi(s^{i-j}) = (-1)^{i-j}$*, then* $(i,j,1,1) \in \mathcal{A}_A$*.*

Proof. Let $\gcd(i,j) = 1$, I be defined as in Theorem 2.2.6, and suppose there exists an evaluation $\psi : A[s,t] \to A$ such that $(\psi \circ f)(i+j) = 0$, $(\psi \circ f)(i+j-1) = \phi(s^{j-1})$, and $(\psi(s^{i-j}) = (-1)^{i-j}$. Then ψ induces a well-defined homomorphism on $\psi^* : M_2(A[s,t]/I) \to M_2(A)$, since $A[s,t]/I$ is not zero by Theorem 2.2.10. Therefore, $(i,j,1,1) \in \mathcal{A}_A$. □

In particular we obtain Lemma 1.7 from [**?**].

Corollary 2.2.12. *Let* k *be an algebraically closed field and* $\gcd(i,j) = 1$*, then* $(i,j,1,1) \in \mathcal{A}_k$*.*

Proof. Suppose the field k is algebraically closed and $\gcd(i,j) = 1$. Then, as seen in case 1 of the proof of Theorem 2.2.10, if $i + j$ is even, then the evaluation $k[s,t]/I \to k$ such that $s \mapsto 1$ and $t \mapsto 0$ satisfies the conditions of Corollary 2.2.11. If $i + j$ is odd and

letting $k[s,t] \to k[t]$ be the evaluation such that $s \mapsto -1$, then, by case 2 of the proof of Theorem 2.2.10, $\bar{f}(i+j)$ and $\bar{f}(i+j-1) - (-1)^{j-1}$ share a common factor. Thus, since k is algebraically closed, there exists a root of this common factor and so there is an evaluation satisfying the conditions of Corollary 2.2.11. Therefore, by Corollary 2.2.11, $(i,j,1,1) \in \mathcal{A}_k$. □

Further, we obtain Theorem 1.5 in [**?**].

Corollary 2.2.13. *Let k be a field, then for all $i,j,n \in \mathbb{N}$, $(i,j,n,n) \in \mathcal{B}_k$.*

Proof. Let k be a field, $\gcd(i,j) = d$, and $i^* = i/d$ and $j^* = j/d$. Then, there exists an algebraic extension L of k such that $I^* = (f(i^*+j^*), f(i^*+j^*-1) - s^{j^*-1}, s^{i^*-j^*} - (-1)^{i^*-j^*})$ has an evaluation that maps I^* to 0 by Corollary 2.2.12. Therefore, letting $w = x^d$ and $z = y^n$, there exists a homomorphism from $L\langle w,z | w^{i^*}y + yw^{j^*} = 1, z^2 = 0\rangle$ to $M_2(L)$ by Corollary 2.2.11. By Lemma 1.2.4, we can embed $M_2(L)$ into $M_M(L)$ so that w has a d-th root and z has an n-th root for some M. Therefore, there is a homomorphism from $L\langle x,y | x^i yn + y^n x^j = 1, y^2 = 0\rangle$ to $M_N(L)$. Further, if $s \mapsto \beta$ and $t \mapsto \alpha$ in L, we can represent α and β as matrices of some size over k, since L is an algebraic extension of k. Therefore, there exists a homomorphism from $R(k;i,j,n,n)$ to $M_N(k)$ for some N so $(i,j,n,n) \in \mathcal{B}_k$. □

2.3 Examples

We conclude this chapter with some interesting examples, the first of which is summarized by the following corollary to Theorem 2.2.6.

Corollary 2.3.1. *Let A be a commutative ring, then $R(A;2,1,1,1) \cong M_2(A)$.*

Proof. We know $R(A;2,1,1,1) \cong M_2(A[s,t]/I)$ where

$$I = (f(3), f(2) - s^0, s^1 - (-1)^1) = (t^2 + s, t - 1, s + 1) = (t - 1, s + 1)$$

and so $A[s,t]/I \cong A$ and therefore $R(A;2,1,1,1) \cong M_2(A)$. $\square$

Example 2.3.2. $R(\mathbb{Q};4,3,1,1)$.

Now consider the specific $\mathbb{Q}$-algebra $R(\mathbb{Q};4,3,1,1)$. Again, using Theorem 2.2.6, we know $R(\mathbb{Q};4,3,1,1) \cong M_2(A[s,t]/I)$ where

$$\begin{aligned} I &= (f(7), f(6) - s^2, s^1 - (-1)^1) \\ &= (t^6 + 5st^4 + 6s^2t^2 + s^3, t^5 + 4st^3 + 3s^2t - s^2, s+1) \\ &= (t^3 - t^2 - 2t + 1, s+1), \end{aligned}$$

since s and -1 are in the same coset and the $\gcd(t^6 - 5t^4 + 6t^2 - 1, t^5 - 4t^3 + 3t - 1) = t^3 - t^2 - 2t + 1$. Since $t^3 - t^2 - 2t + 1$ is irreducible over $\mathbb{Q}$, then $\mathbb{Q}[s,t]/I$ is a field extension of $\mathbb{Q}$ given by $\mathbb{Q}(\lambda)$ where λ satisfies the polynomial $\lambda^3 - \lambda^2 - 2\lambda + 1$. This example is important because it answers questions about the structure of $R(A;i,j,1,1)$ as a matrix ring and its underlying ring when i and j are relatively prime.

First, $A[s,t]/I$ depends very much on the choice of A. When $A = \mathbb{Q}$, then $A[s,t]/I$ is a field. However, if $\mathbb{Q}$ were replaced with a ring where $t^3 - t^2 - 2t + 1$ was reducible, the underlying ring would no longer be a domain, let alone a field.

Next, while $R(\mathbb{Q};4,3,1,1) \cong M_2(\mathbb{Q}(\lambda))$, we still have $(4,3,1,1) \notin \mathcal{A}_{\mathbb{Q}}$. There are numerous ways to see this. There is no non-trivial homomorphism that maps a field extension to its base field. This is the case since 1 must map to 1 and hence $\mathbb{Q}$ maps to $\mathbb{Q}$. This leaves no option to map λ to a rational number. Therefore, there is no non-trivial homomorphism $M_2(\mathbb{Q}(\lambda)) \to M_2(\mathbb{Q})$. Another way to see this, and most importantly for the next chapter, $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ does not have any quadratic factors over $\mathbb{Q}$ ($x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbb{Q}$). By Lemma 2.1.6, we have for x in $R(\mathbb{Q};4,3,1,1)$ that $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 = 0$. Suppose $\phi : R(\mathbb{Q};4,3,1,1) \to M_2(\mathbb{Q})$

is a ring homomorphism. In $M_2(\mathbb{Q})$, the image of x would satisfy some quadratic polynomial, $\phi(x)^2 - a\phi(x) + b = 0$, namely its characteristic polynomial in $M_2(\mathbb{Q})$. Therefore $x^2 - ax + b \in \ker(\phi)$. But $\gcd(x^6 - x^5 + x^4 - x^3 + x^2 - x + 1, x^2 - ax + b) = 1$ for all $a, b \in \mathbb{Q}$. Therefore, $\ker(\phi) = R(\mathbb{Q}; 4, 3, 1, 1)$ and $\phi(1) = 0$, which is a contradiction to ϕ being a homomorphism.

Since, $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ is irreducible over $\mathbb{Q}$, the matrix ring $M_6(\mathbb{Q})$ is the smallest matrix ring $R(\mathbb{Q}; 4, 3, 1, 1)$ can be mapped to non-trivially. Since, every field extension is a vector space over its base ring and every element of a field extension acts linearly on that vector space by multiplication; every field extension can be realized as set of matrices of dimension equal to the degree of the extension. Therefore, $\mathbb{Q}(\lambda)$ is isomorphic to a subring of $M_3(\mathbb{Q})$. This gives an explicit isomorphism from $M_2(\mathbb{Q}(\lambda))$ to a subring of $M_2(M_3(\mathbb{Q})) = M_6(\mathbb{Q})$. This agrees with Corollary 2.2.13.

Example 2.3.3. $R(A; 1, 1, 1, 1)$.

For our third example, let A be a commutative ring and consider $R(A; 1, 1, 1, 1)$. Now, we can show that $\{yx = 1 - xy, y^2 = 0\}$ forms a complete set of reductions in $R(A; 1, 1, 1, 1)$ under the deglex order. This means that, as a free A-module with basis given by the set $\{1, x, x^2, \ldots, y, xy, x^2y, \ldots\}$, $R(A; 1, 1, 1, 1)$ is infinite rank over A (as there is no reduction for x^n). Using Theorem 2.2.6 we have $R(A; 1, 1, 1, 1) \cong M_2(A[s])$ since

$$I = (f(2), f(1) - s^0, s^0 - (-1)^0) = (t).$$

However, in the following example, we will not have the use of Theorem 2.2.6 and so we will develop a different technique for analysis. A priori it is hard to see how an infinite-rank A-module can be a finite-rank matrix ring. This isomorphism is more obvious by introducing a new variable to our relation system. Let $x^2 = s$, giving us $k\langle x, y, s | xy + yx = 1, y^2 = 0, x^2 = s\rangle$. This gives the following set of reductions $\{yx = 1 - xy, y^2 = 0, x^2 = s\}$, which

is not complete in the spirit of the Diamond Lemma, Theorem 1.2.9. This set of reductions has the ambiguities yx^2 and x^3. By adding reductive relations resolving the ambiguities these yield, we are left with the complete reduction system $\{yx = 1 - xy, y^2 = 0, x^2 = s, xs = sx, ys = sy\}$ under the deglex order. Therefore, s is in the center of $R(k; 1, 1, 1, 1)$. Since s is in the center of $R(A; 1, 1, 1, 1)$, then $R(A; 1, 1, 1, 1)$ is an $A[s]$-algebra and, by our reduction system a free $A[s]$-module. As an $A[s]$-module, it has basis $\{1, x, y, xy\}$ and thus is rank 4. Now $R(A; 1, 1, 1, 1)$ has the set of 2×2 matrix units

$$e_{11} = 1 - xy,\ e_{12} = y,\ e_{21} = x - sy,\ e_{22} = xy$$

which shows $R(A; 1, 1, 1, 1) \cong M_2(T)$ for some $A[s]$-algebra T. But both $R(A; 1, 1, 1, 1)$ and $M_2(T)$ have rank 4 over $A[s]$ and so $T = A[s]$. Therefore $R(A; 1, 1, 1, 1) \cong M_2(A[s])$ as $A[s]$-algebras, which is our infinite-rank A-algebra.

Example 2.3.4. $R = R(\mathbb{F}_2; 2, 2, 1, 1)$.

For our final example, we consider $R = R(\mathbb{F}_2; 2, 2, 1, 1)$. Here, we cannot use Theorem 2.2.6 to analyze this algebra since $\gcd(2, 2) = 2$. This algebra, however, is very similar to our previous example. As in Example 2.3.3 $yx^2 = 1 + x^2y$ and $y^2 = 0$ form a complete reduction system (just doubling the exponent on x). Here, R is an infinite-dimensional $\mathbb{F}_2$-vector space. There are two problems; x^n and $(yx)^n$ are both irreducible. By our previous example, $R(\mathbb{F}_2; 2, 2, 1, 1)$ contains a subring isomorphic to $M_2(A([s])$ generated by x^2 and y. If we could find a square root of x, we would have a description of R. This, however, is not possible and is summarized in the following theorem.

Proposition 2.3.5. *The matrix* $X = \begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix}$ *does not have a square root in* $M_2(\mathbb{F}_2[s])$.

Proof. If X has a square root, then there exist $a, b, c, d \in \mathbb{F}_2[s]$ that satisfy the equations

$$a^2 + bc = 0,\ ab + bd = s,\ ac + cd = 1,\ d^2 + bc = 0$$

This means that $b(a+d) = 1$ and thus $a+d$ is a unit and $a+d = 1$. Therefore, $a^2+d^2 = 1$. However, using the first and fourth relation we get $a^2 = d^2$, and this is not possible. Therefore, X does not have a square root in $M_2(\mathbb{F}_2[s])$. □

This shows that $(2,2,1,1) \notin \mathcal{A}_{\mathbb{F}_2}$. The following theorem is a generalization of this result.

Theorem 2.3.6. *Let A be a commutative ring. There is no non-trivial homomorphism from $R(\mathbb{F}_2; 2,2,1,1)$ to $M_2(A)$ or $M_3(A)$.*

Proof. We will begin by showing there is no homomorphism $R \to M_2(A)$. Assume $\phi : R \to M_2(A)$ is such a homomorphism. Since $\phi(2) = \phi(0) = 0$, A must have characteristic 2. Let $\phi(x) = X$ and $\phi(y) = Y$ be the image of x and y respectively. Then, X must satisfy a monic quadratic polynomial with coefficients from A. Therefore, there exist $a, b \in A$ such that $X^2 + aX + b = 0$. Now, we also have $X^2Y + YX^2 = 1$. In the spirit of the Diamond Lemma, we want to find relations in $M_2(A)$. From the reduction system $\{YX^2 = 1+X^2Y, Y^2 = 0, X^2 = aX+b\}$, which is not complete, and resolving the ambiguity $YX^2 = Y(X^2)$, we obtain the system $\{aYX = 1 + aXY, Y^2 = 0, X^2 = aX + b\}$. However, we now have a new ambiguity $aYX^2 = (aYX)X = a(YX^2)$. Resolving this ambiguity yields $a = 0$ which implies $0 = 1$ from $aYX = 1 + aXY$, which of course collapses our ring to the trivial ring. This is a contradiction to ϕ being a homomorphism.

Next, assume $\phi : R \to M_3(A)$ is a homomorphism. Again, A must have characteristic 2 and the image of x must now satisfy a monic cubic polynomial with coefficients in A. Let $\phi(x) = X$ and $\phi(y) = Y$ be the image of x and y respectively. Again, we have a new reduction, $X^3 = aX^2 + bX + c$ where $a, b, c \in A$ and a new ambiguity, YX^3:

$$YX^3 = Y(X^3) = Y(aX^2 + bX + c)$$

on one hand and

$$YX^3 = (YX^2)X = (1 + X^2Y)X = X + X^2YX$$

on the other. By resolving this YX^3 we achieve a new reduction

$$X^2YX = a + X + aX^2Y + bYX + cY.$$

Resolving the ambiguity X^3YX:

$$\begin{aligned} X^3YX &= X(X^2YX) \\ &= X(a + X + aX^2Y + bYX + cY) \\ &= aX + X^2 + a(X^3)Y + bXYX + cXY \\ &= aX + X^2 + a(aX^2 + bX + c)Y + bXYX + cXY \\ &= aX + X^2 + a^2X^2Y + (ab + c)XY + acY + bXYX \end{aligned}$$

on one hand, and

$$\begin{aligned} X^3YX &= (X^3)YX \\ &= (aX^2 + bX + c)YX \\ &= a(X^2YX) + bXYX + cYX \\ &= a(a + X + aX^2Y + bYX + cY) + bXYX + cYX \\ &= a^2 + aX + a^2X^2Y + (ab + c)YX + acY + bXYX \end{aligned}$$

on the other. So we obtain the relation

$$(ab + c)YX = a^2 + X^2 + (ab + c)XY.$$

Finally, using the ambiguity $(ab+c)YX^2$:

$$\begin{aligned}(ab+c)YX^2 &= ((ab+c)YX)X \\ &= (a^2+X^2+(ab+c)XY)X \\ &= a^2X+X^3+(ab+c)XYX \\ &= a^2X+X^3+X((ab+c)YX) \\ &= a^2X+X^3+X(a^2+X^2+(ab+c)XY) \\ &= (ab+c)XY\end{aligned}$$

on one hand, and

$$(ab+c)YX^2 = (ab+c)(YX^2) = (ab+c)(1+X^2Y) = (ab+c)+(ab+c)X^2Y$$

on the other, we find that $ab+c=0$. Substituting this in our most recent reduction, we see that $X^2=a^2$ and finally that

$$1 = X^2Y+YX^2 = a^2Y+Ya^2 = 2a^2Y = 0,$$

contradicting that ϕ is a homomorphism. □

However, we are able to find a homomorphism from R to $M_4(\mathbb{F}_2[s])$. Using Lemma

1.2.4, we can embed $M_2(\mathbb{F}_2[s])$ into $M_4(\mathbb{F}_2[s])$ and give x a square root in the following way

$$x = \begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix} \text{ and } y = \begin{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{pmatrix}$$

We will show that this is the "best" way we can map $R = R(\mathbb{F}_2; 2, 2, 1, 1)$ to a 4×4 matrix ring in a sense that we will see shortly. We have seen that when $\gcd(i, j) = 1$, $R(A; i, j, 1, 1)$ is isomorphic to a complete matrix ring over a commutative ring. Our next theorem will show that if $\gcd(i, j) \neq 1$, this is not necessarily the case.

Theorem 2.3.7. *Let $R = R(\mathbb{F}_2; 2, 2, 1, 1)$, then R is not isomorphic to a complete matrix ring over a commutative ring A.*

Proof. We will analyze R in the same way we analyzed Example 2.3.3. First we will introduce a new variable s and the reduction $x^4 = s$. Now, if $R \cong M_4(A)$ for some commutative ring A, then this would imply that there exist a, b, c, and d in the preimage of A under the isomorphism such that $(yx)^4 + a(yx)^3 + b(yx)^2 + c(yx) + d = 0$ since every matrix satisfies its characteristic equation in a matrix ring over a commutative ring. However, there is no reduction for $(yx)^n$ and so we look at $(yx)^4x + a(yx)^3x + b(yx)^2x + c(yx)x + dx = 0$ since there is a reduction for yx^2. Using these reductions we see $b = yxyx + xyxy + y$, which, actually, is in the center of R. So we introduce the new variable b as defined above. We now have the reduction system $\{yx^2 = 1 + x^2y, y^2 = 0, x^4 = s, yxyx = b + y + xyxy\}$, which is not complete. It gives rise to the complete reduction system

$$\{yx^2 = 1 + x^2y, y^2 = 0, x^4 = s, yxyx = b + y + xyxy,$$

$$xs = sx, ys = sy, xb = bx, yb = by, sb = bs\} \tag{2.7}$$

under the deglex order; which is the same reduction system with the added reductions showing b and s are in the center of R. Using these reductions, we see that an element in R can be written uniquely as a linear combination of the set of irreducible monomials/words

$$\mathcal{B} = \{1, x, x^2, x^3, y, xy, x^2y, x^3y, yx, xyx, x^2yx, x^3yx, yxy, xyxy, x^2yxyx, x^3yxy\} \tag{2.8}$$

with coefficients from $\mathbb{F}_2[b, s]$. So R is a free $\mathbb{F}_2[b, s]$-module of rank 16.

Now, we want to find the center of R. We know $R \cong M_2(T)$ for some $\mathbb{F}_2$-algebra T with matrix units $e_{11} = 1 + x^2y$, $e_{12} = y$, $e_{21} = x^2 + sy$, $e_{22} = x^2y$. We can find T with the map $r \mapsto e_{11}re_{11} + e_{21}re_{12}$ where $r \in R$. Under this map, the center of R will be fixed, since if $z \in Z(R)$, then

$$z \mapsto e_{11}ze_{11} + e_{21}ze_{12} = z(e_{11}e_{11} + e_{21}e_{12}) = z$$

Since $b, s \in Z(R)$, we only need to find the image of $\mathcal{B}$, which is

$$\{0, 1, x + x^2yx + x^3y, sxy + syx, xy + yx, xyx + x^2y + bx^2, sb\}$$

Therefore, $T = \text{span}_{\mathbb{F}_2[b,s]}\left(\{1, x + x^2yx + x^3y, xy + yx, xyx + x^2y + bx^2\}\right)$. Now, if $z \in Z(R)$, z must be a linear combination of these elements. Let $p_0, p_1, p_2, p_3 \in \mathbb{F}_2[b, s]$ and suppose

$$z = p_0 1 + p_1(x + x^2yx + x^3y) + p_2(xy + yx) + p_3(xyx + x^2y + bx^2)$$

and $zx = xz$. Reducing each side of $zx = xz$, we see that $p_1 = p_2 = p_3 = 0$. Therefore, the only elements in $Z(R)$ are polynomials of b and s.

Now, suppose $R \cong M_N(A)$ as an $\mathbb{F}_2$ algebra for some commutative ring A and natural number N. Then $A \cong Z(R) = \mathbb{F}_2[b, s]$. Since R has rank 16 as a free $\mathbb{F}_2[b, s]$-module, then $N = 4$. Therefore, every element of R must satisfy a monic, fourth-degree polynomial with coefficients from $\mathbb{F}_2[b, s]$. In fact, every of element of $\mathcal{B}$ does satisfy a monic, fourth-degree

polynomial. However, $xy + x$ does not: using our reduction system we obtain

$$(xy + x)^4 = bxyxy + s$$

$$(xy + x)^3 = bxy + x^2yxy + xy + by + x^3y + x^3$$

$$(xy + x)^2 = xyxy + x^2$$

$$(xy + x)^1 = xy + x.$$

Now let $q_0, q_1, q_2, q_3 \in \mathbb{F}_2[b, s]$ and suppose $(xy + x)^4 = q_3(xy + x)^3 + q_2(xy + x)^2 + q_1(xy + x) + q_0$. Since $(xy + x)$ is the only term that has a non-zero coefficient on x, then $q_1 = 0$. Similarly, $q_2 = 0$ and $q_3 = 0$. But then we have $bxyxy + s = q_0$, which is not possible since R is a free $\mathbb{F}_2[b, s]$-module and $xyxy$ is irreducible. Therefore, $xy + y$ does not satisfy a monic, fourth-degree polynomial. This means that R cannot be isomorphic to a complete matrix ring over a commutative ring, unless $bxyxy = 0$. □

We now consider R with the reduction system (2.7) with the added relation $bxyxy = 0$. We resolve the ambiguity $byxyxy$:

$$byxyxy = y(bxyxy) = 0$$

on one hand, and

$$byxyxy = b(yxyx)y = b(b + y + xyxy)y = b^2y + by^2 + bxyxy^2 = b^2y$$

on the other. So we obtain the relation, $b^2y = 0$. Next, we resolve the ambiguity b^2yx^2: on one hand we have

$$b^2yx^2 = (b^2y)x^2 = 0$$

and on the other

$$b^2yx^2 = b^2(yx^2) = b^2(1 + x^2y) = b^2 + b^2x^2y = b^2 + x^2(b^2y) = b^2$$

and so we obtain $b^2 = 0$. We resolve the ambiguity $bxyxyx$ next:

$$bxyxyx = (bxyxy)x = 0$$

on one hand and

$$bxyxyx = bx(yxyx) = bx(b + y + xyxy) = b^2x + bxy + x(bxyxy) = (b^2)x + bxy = bxy$$

on the other and so we obtain $bxy = 0$. This leads to the ambiguity $byxyx$, which gives the following two relations:

$$byxyx = y(bxy)xy = 0$$

and

$$byxyx = b(yxyx) = b(b + y + xyxy) = b^2 + by + bxyxy = by$$

and so we get $by = 0$. Finally, we consider the ambiguity byx^2, from which we obtain the following two equations

$$byx^2 = (by)x^2 = 0$$

and

$$byx^2 = b(yx^2) = b(1 + x^2y) = b + bx^2y = b + x^2(by) = b.$$

And thus, $b = 0$.

Suppose we have a map $\phi : R \to M_4(A)$ for some commutative ring A. From the proof of Theorem 2.3.7, we know $\phi(bxyxy) = 0$ and from above, $\phi(b) = 0$. Now, consider $R/(b)$ where (b) is the two-sided ideal generated by b. Let $\bar{x}$ and $\bar{y}$ be the image of x and y in this quotient ring respectively. In this quotient ring, the set $\{\bar{y}\bar{x}\bar{y}, \bar{x}\bar{y}\bar{x}\bar{y}, \bar{x}^2\bar{y}\bar{x}\bar{y}, \bar{x}^3\bar{y}\bar{x}\bar{y}\}$ is

invariant under left multiplication by $\bar{x}$ and $\bar{y}$ and thus is invariant under the action of left multiplication by $R/(b)$. Under this action we can realize $R/(b)$ as a set of 4×4 matrices where

$$\bar{x} = \begin{pmatrix} 0 & 0 & 0 & s \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } \bar{y} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which is a permutation of the representation we found at the beginning of this example. Under this quotient map, the image of (2.8) is a linearly independent set over $\mathbb{F}_2[s]$ and so $R/(b) \cong M_4(\mathbb{F}_2[s])$.

Proposition 2.3.8. *For $R = R(\mathbb{F}_2; 2, 2, 1, 1)$, $b = y + xyxy + yxyx$ and A a commutative ring, if $\phi : R \to M_4(A)$, then $\phi(b) = 0$ and the quotient ring $R/(b) \cong M_2(\mathbb{F}_2[s])$ where $s = x^4$.*

In particular, R is isomorphic to a 2×2 matrix ring over some non-commutative $\mathbb{F}_2$-algebra by Theorem 2.2.1 and Theorem 2.3.6, such that when quotiented by (b) is isomorphic to a 4×4 matrix ring over a commutative ring. This is the "best" map we mentioned earlier. In fact, we can see that the following elements form a complete set of 4×4 matrix units:

$$e_{11} = 1 + xyx + x^3yxy, \qquad e_{12} = yx + xy + x^2yxy,$$

$$e_{13} = y + xyxy, \qquad e_{14} = yxy,$$

$$e_{21} = x + x^2yx + syxy, \qquad e_{22} = xyx + x^2y + x^3yxy,$$

$$e_{23} = xy + x^2yxy, \qquad e_{24} = xyxy,$$

$$e_{31} = x^2 + x^3yx + sxyxy, \qquad e_{32} = x^2yx + x^3y + syxy,$$

$$e_{33} = x^2y + x^3yxy, \qquad e_{34} = x^2yxy,$$

$$e_{41} = x^3 + syx + sx^2yxy, \qquad e_{42} = x^3yx + sy + sxyxy,$$

$$e_{43} = x^3y + syxy, \qquad e_{44} = x^3yxy.$$

Finally, we remark the set $\{y, xy, x^2y, x^3y, yxy, xyxy, x^2yxy, x^3yxy\}$, is invariant under left multiplication by R. Under this left-multiplication action, we can write x and y as 8×8 matrices

$$x = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & s & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & s \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \text{ and } y = \left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & b & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Under this map, (2.8) is linearly independent and thus we can realize R as a subset of $M_8(\mathbb{F}_2[b, s])$. (Note: if we let $b = 0$, in the last four columns of these matrices, only the last four rows have non-zero entries. Then $\{yxy, xyxy, x^2yxy, x^3yxy\}$ is invariant under x and y.)

This example raises the question: for $R(A; i, j, m, n)$, is it always possible to find a commutative A-algebra T, such that $R(A; i, j, m, n)$ can be embedded in $M_N(T)$ for some N? Currently, there are only partial answers to this question.

Chapter 3: Finding $\mathcal{A}_k$ for Fields when $m = n = 1$

In the previous chapter we showed that if $\gcd(i, j) = 1$, then $R(A; i, j, 1, 1) \cong M_2(A[s, t]/I)$ (see Theorem 2.2.6). However, we also showed that just because $R(A; i, j, 1, 1) \cong M_2(T)$ for some commutative ring T, does not necessarily mean that $(i, j, 1, 1) \in \mathcal{A}_A$ (see Example 2.3.2). In this chapter, we will restrict our attention to $R(k; i, j, 1, 1)$ where k is a field and investigate the set $\mathcal{A}_k \in \mathbb{N}^4$ for various k.

3.1 Defining Sequences and Sequence Conditions

Let $\phi : R(k; i, j, 1, 1) \to M_2(k)$ and let $\phi(x) = X$ and $\phi(y) = Y$. Since X satisfies its characteristic polynomial, there exist $a, b \in k$ such that $X^2 - aX + b = 0$ where $a = \text{tr}(X)$ and $b = \det(X)$, and so, $x^2 - ax + b \in \ker(\phi)$. Therefore, it makes sense to impose a characteristic polynomial on x.

Definition 3.1.1. *For a field k let*

$$S(k; i, j, a, b) = k\langle x, y | x^i y + y x^j = 1, y^2 = 0, x^2 = ax - b\rangle$$

$$= R(i, j, 1, 1)/(x^2 - ax + b).$$

In the above definition, $S(k; i, j, a, b)$ is $R(k; i, j, 1, 1)$ with the added relation of a characteristic equation for x.

Definition 3.1.2. *Let $g : \mathbb{N}_0 \to k$ be defined recursively as $g(n) = ag(n-1) - bg(n-2)$ where $g(0) = 0$ and $g(1) = 1$.*

This function will play an important roll in this chapter. This should not be a surprise as the similar recursive function $f : A[s, t] \to A$ as defined in Definition 2.2.4 played a major

role in Theorem 2.2.6. Unless otherwise state, for the rest of his chapter g will always be the function corresponding to $a, b \in k$ for $S(k; i, j, a, b)$ as defined in Definition 3.1.1.

Lemma 3.1.3. *If $x^2 = ax - b$, then $x^n = g(n)x - bg(n-1)$ for $n \geq 1$.*

Proof. This will be a proof by induction on n. Let $n = 1$, then $x^1 = 1x - 0 = g(1)x - bg(0)$. Assume that $x^n = g(n)x - bg(n-1)$. Then

$$\begin{aligned} x^{n+1} &= xx^n \\ &= x(g(n)x - bg(n-1)) \\ &= g(n)x^2 - bg(n-1)x \\ &= g(n)(ax - b) - bg(n-1)x \\ &= (ag(n) - bg(n-1))x - bg(n) \\ &= g(n+1)x - bg(n). \end{aligned}$$

□

Theorem 3.1.4. *Let $a, b \in k$, then $S(k; i, j, a, b) \cong M_2(k)$ or $S(k; i, j, a, b) = 0$.*

Proof. Suppose $S(k; i, j, a, b) \neq \{0\}$. We have from Theorem 2.2.1 that $e_{11} = 1 - x^i y$, $e_{12} = y$, $e_{21} = x^i y x^j$, $e_{22} = x^i y$ is a set of 2×2 matrix units. Therefore, $S(k; i, j, a, b) \cong M_2(T)$ for some k-algebra T and, since $S(k; i, j, a, b) \neq \{0\}$, then $\{e_{11}, e_{12}, e_{21}, e_{22}\}$ is a linearly independent set over k. In $S(k; i, j, a, b)$, we have that $x^2 = ax - b$. Using Lemma 3.1.3, we get $x^i = g(i)x - bg(i-1)$ and $x^j = g(j)x - bg(j-1)$. Note that if $g(j) = 0$ then $x^j = bg(j-1) \in k$ and so $1 = x^i y + y x^j = x^i y + y bg(j-1)$ and hence $y = x^i y^2 + bg(j-1)y^2 = 0$ and so $1 = 0$ and hence $S(k; i, j, a, b)$ is trivial. Thus, since $S(k; i, j, a, b)$ is not trivial, $g(j) \neq 0$. Along with the relation $x^i y + y x^j = 1$ we have that $g(i)xy - bg(i-1)y + g(j)yx - bf(j-1)y = 1$.

And so we get $g(j)yx = 1 + (bg(i-1) + bg(j-1))y - g(i)xy$ and hence

$$yx = \frac{1}{g(j)} + \frac{bg(i-1) + g(j-1)}{g(j)}y - \frac{g(i)}{g(j)}xy. \tag{3.1}$$

This equation, together with $x^2 = ax - b$ and $y^2 = 0$ shows that $S(k; i, j, a, b) = \text{span}_k(\{1, x, y, xy\})$ and so $\dim_k(S(k; i, j, a, b)) \leq 4$. Since $S(k; i, j, a, b)$ is a non-trivial 2×2 matrix algebra over k, $\dim_k(S(k; i, j, a, b)) \geq 4$. Thus, $\dim_k(S(k; i, j, a, b)) = 4$ and therefore $S(k; i, j, a, b) \cong M_2(k)$. □

We have now shown that with a correct choice of $a, b \in k$, we have $S(k; i, j, a, b) \cong M_2(k)$. Our goal now will be to find the $a, b \in k$ that will work for a given i and j. We begin with a general lemma about 2×2 matrices over a field k.

Lemma 3.1.5. *For a field k and $X, Y \in M_2(k)$, then there exists $c \in k$ such that*

$$YX = c \cdot I + \text{tr}(X) \cdot Y + \text{tr}(Y) \cdot X - XY$$

Proof. Let

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } Y = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Then we have

$$\text{tr}(X)Y = \begin{pmatrix} ap + dp & aq + dq \\ ar + dr & as + ds \end{pmatrix}, \text{tr}(Y)X = \begin{pmatrix} ap + as & bp + bs \\ cp + cs & dp + ds \end{pmatrix},$$

$$XY = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}, YX = \begin{pmatrix} ap + cq & bp + dq \\ ar + cs & br + ds \end{pmatrix},$$

and hence

$$X + XY - \mathrm{tr}(X)Y - \mathrm{tr}(Y)X = \begin{pmatrix} cq + br - as - dp & 0 \\ 0 & cq + br - as - dp \end{pmatrix}$$

$$= (cq + br - as - dp) \cdot I.$$

□

The following theorem will show when $S(k; i, j, a, b) \cong M_2(k)$.

Theorem 3.1.6. *For $S(k; i, j, a, b)$ as defined in Definition 3.1.1, we have $S(k; i, j, a, b) \cong M_2(k)$ if and only if $g(j) \neq 0$, $g(i) = g(j)$, and $g(j + 1) = bg(i - 1)$.*

Proof. ($\Rightarrow$): Suppose $S(k; i, j, a, b) \cong M_2(k)$. From the proof of Theorem 3.1.4, we have $g(j) \neq 0$. We also have in $M_2(k)$ that $x^2 = \mathrm{tr}(x) \cdot x - \det(x)$, since x satisfies its characteristic polynomial. From the proof of Theorem 3.1.4, we have that $\{1, x, y, xy\}$ is a linearly independent set. Therefore, since $x^2 = ax - b$ and $y^2 = 0$, $\mathrm{tr}(x) = a$, $\det(x) = b$, $\mathrm{tr}(y) = 0$, and $\det(y) = 0$. Therefore, by Lemma 3.1.5, we get $yx = c \cdot 1 + a \cdot y - xy$ for some $c \in k$ and by equation (3.1), we also have

$$yx = \frac{1}{g(j)} + \frac{bg(i-1) + bg(j-1)}{g(j)} y - \frac{g(i)}{g(j)} xy.$$

Since $\{1, x, y, xy\}$ is a linearly independent set, we have

$$c = \frac{1}{g(j)},\ a = \frac{bg(i-1) + bg(j-1)}{g(j)},\ 1 = \frac{g(i)}{g(j)}.$$

Therefore, $g(j) = g(i)$ and $ag(j) = bg(i-1) + bg(j-1)$, which implies that $g(j+1) = bg(i-1)$.

($\Leftarrow$): Assume $g(j) \neq 0$, $g(i) = g(j)$, and $g(j+1) = bg(i-1)$. If

$$X = \begin{pmatrix} 0 & -bg(j) \\ 1/g(j) & a \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

then

$$aX - b = \begin{pmatrix} 0 & -abg(j) \\ a/g(j) & a^2 \end{pmatrix} - \begin{pmatrix} -b & 0 \\ 0 & -b \end{pmatrix} = \begin{pmatrix} -b & -abg(j) \\ a/g(j) & a^2 - b \end{pmatrix} = X^2.$$

By Lemma 3.1.3, we then get

$$X^i = g(i)X - bg(i-1) = g(j)X - g(j+1) = \begin{pmatrix} -g(j+1) & -bg(j)^2 \\ 1 & bg(j-1) \end{pmatrix},$$

and

$$X^j = g(j)X - bg(j-1) = \begin{pmatrix} -bg(j-1) & -bg(j)^2 \\ 1 & g(j+1) \end{pmatrix},$$

and so

$$\begin{aligned} X^iY + YX^j &= \begin{pmatrix} 0 & -g(j+1) \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & g(j+1) \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= 1, \end{aligned}$$

and

$$Y^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Therefore, X and Y satisfy the relations of $S(k;i,j,a,b)$ and so $S(k;i,j,a,b) \neq \{0\}$ and thus $S(k;i,j,a,b) \cong M_2(k)$ by Theorem 3.1.4. □

Note that by Theorem 2.1.4, We have that $R(k;i,j,1,1) = R(k;j,i,1,1)$, and therefore $S(k;i,j,a,b) = S(k;j,i,a,b)$. Thus, if $S(k;i,j,a,b)$ is non-trivial, we get $bg(j-1) = g(i+1)$.

Before moving on, we treat a special case of $S(k;i,j,a,b)$.

Theorem 3.1.7. *For a field k, $S(k;i,j,a,0)$ is non-trivial if and only if $a = 0$ and $i = j = 1$.*

Proof. Suppose $S(k;i,j,a,b)$ is non-trivial and $b = 0$. Then $g(n) = ag(n-1)$ with $g(0) = 0$ and $g(1) = 1$. This recursive relation has explicit formula $g(n) = a^{n-1}$ for $n \geq 1$, therefore, since $b = 0$, we have $a^j = g(j+1) = bg(j-1) = 0$. Thus $a = 0$ since k is a field. Therefore, $g(n) = 0$ for all $n \neq 1$ with $g(1) = 1$. Since $S(k;i,j,a,b)$ is non-trivial, by Theorem 3.1.6 $g(j) \neq 0$ and so $j = 1$. Since $g(j) = g(i)$, by Theorem 3.1.6, $i = 1$ as well. □

In the previous chapter, we found relations on the function $f : \mathbb{N}_0 \to A[s,t]$, defined in Definition 2.2.4, that defined the underlying ring of $R(k;i,j,1,1)$ when $\gcd(i,j) = 1$. The following theorem relates the generators of the ideal I, defined in Theorem 2.2.6 to the relations found in Theorem 3.1.6. First, however, we need a technical lemma.

Lemma 3.1.8. *Let $r, s \in k$. If $rg(m) = sg(n)$ and $rg(m+1) = bsg(n-1)$, then $rg(m+2) = b^2sg(n-2)$ and $brg(m-1) = sg(n+1)$.*

Proof. The above lemma can be easily seen with the definition of g and the following equations

$$rg(m+2) = arg(m+1) - brg(m)$$

$$= absg(n-1) - brg(n)$$

$$= b^2 rg(n-2),$$

$$sg(n+1) = asg(n) - bsg(n-1)$$

$$= arg(m) - rg(m+1)$$

$$= bsg(m-1).$$

□

This lemma will allow us to shift the argument of g by increasing or decreasing powers of b.

Theorem 3.1.9. *Suppose $b \neq 0$ and $g(j) \neq 0$, then $g(i) = g(j)$ and $g(j+1) = bg(i-1)$ if and only if $g(i+j) = 0$, $g(i+j-1) = b^{j-1}$, and $b^{i-j} = 1$.*

Proof. ($\Rightarrow$): Suppose $g(i) = g(j)$ and $g(j+1) = bg(i-1)$. Then, by repeated use of Lemma 3.1.8, we get that $g(i+j) = b^j g(0) = 0$, $g(i+j-1) = b^{j-1}g(1) = b^{j-1}$, and $g(i+j-1) = b^{i-1}g(1) = b^{i-1}$. Since $b^{j-1} = b^{i-1}$, then $b^{i-j} = 1$.
($\Leftarrow$): Suppose $g(i+j) = 0$, $g(i+j-1) = b^{j-1}$, and $b^{i-j} = 1$. Then $g(i+j) = b^j g(0)$, $g(i+j-1) = b^{j-1}g(1)$, and $b^i = b^j$. Then, using Lemma 3.1.8 again, we have $b^j g(i) = b^j g(j)$ and $b^{j+1}g(i-1) = b^j g(j+1)$. Since $b \neq 0$, then $g(i) = g(j)$ and $g(j+1) = bg(i-1)$. □

We saw in the previous chapter by Corollary 2.2.11 that if $\gcd(i,j) = 1$ and $A[s,t]$ has an evaluation $\phi : A[s,t] \to A$ such that $(\phi \circ f)(i+j) = 0$, $(\phi \circ f)(i+j-1) = \phi(s^{j-1})$, and $\phi(s^{i-j}) = (-1)^{i-j}$, then $(i,j,1,1) \in \mathcal{A}_k$ where $f : \mathbb{N}_0 \to A[s,t]$ is defined as in Definition 2.2.4. We will now show that the converse is also true for $A = k$ where k is a field.

Theorem 3.1.10. *Let k be a field and $f : k[s,t] \to k$ be such that $f(0) = 0$, $f(1) = 1$ and $f(n) = tf(n-1) + sf(n-2)$ for $n \geq 2$ as defined in Definition 2.2.4. If $(i,j,1,1) \in$*

$\mathcal{A}_k$ and $\gcd(i,j) = 1$*, then there exists an evaluation of* $k[s,t]$ $\phi : k[s,t] \to k$ *such that* $(\phi \circ f)(i+j) = 0$*,* $(\phi \circ f)(i+j-1) = \phi(s^{j-1})$*, and* $\phi(s^{i-j} - (-1)^{i-j}) = 0$*.*

Proof. Suppose $(i,j,1,1) \in \mathcal{A}_k$ and $\gcd(i,j) = 1$. By Theorem 2.1.4 we have $R(k;i,j,1,1) = R(k;j,i,1,1)$ and so $(i,j,1,1) \in \mathcal{A}_k$ if and only if $(j,i,1,1) \in \mathcal{A}_k$. Hence, since $\gcd(i,j) = 1$, we may assume j is odd. By Theorem 3.1.6, there exist $a, b \in k$ such that $g(i) = g(j)$, $g(j) \neq 0$, and $g(j+1) = bg(i-1)$. Let $\phi : k[s,t] \to k$ be the evaluation such that $s \mapsto -b$ and $t \mapsto a$. Since $g : k \to k$ is defined as $g(0) = 0$, $g(1) = 1$, and $g(n) = ag(n-1) - bg(n-2)$, then $\phi \circ f = g$. Suppose $b \neq 0$, then by Theorem 3.1.9, we have $g(i+j) = 0$, $g(i+j-1) = b^{j-1}$, and $b^{i-j} = 1$ and so

$$\begin{aligned}
(\phi \circ f)(i+j) &= g(i+j) \\
&= 0, \\
(\phi \circ f)(i+j-1) &= g(i+j-1) \\
&= b^{j-1} \\
&= (-b)^{j-1} \\
&= \phi(s^{j-1}), \\
\phi(s^{i-j} - 1^{i-j}) &= (-b)^{i-j} - (-1)^{i-j} \\
&= (-1)^{i-j} b^{i-j} - (-1)^{i-j} \\
&= (-1)^{i-j} - (-1)^{i-j} \\
&= 0,
\end{aligned}$$

since j is odd. Therefore, ϕ meets the requirements above. Suppose $b = 0$, then by Theorem 3.1.7, $a = 0$, $i = j = 1$, and $g(1) = 1$ and $g(n) = 0$ for $n \neq 1$ and so $\phi(s) = \phi(t) = 0$.

Therefore, we have

$$\begin{aligned}(\phi \circ f)(i+j) &= g(2)\\ &= 0,\\ (\phi \circ f)(i+j-1) &= g(1)\\ &= 1\\ &= \phi(s^{1-1}),\\ \phi(s^{i-j} - 1^{i-j}) &= \phi(s^0 - 1)\\ &= \phi(1-1)\\ &= \phi(0)\\ &= 0,\end{aligned}$$

and so ϕ meets the requirement above. □

Theorem 3.1.10 shows us that the relations we found in Theorem 3.1.6 that allow us to show when $(i, j, 1, 1) \in \mathcal{A}_k$ are a generalization of those we found in Theorem 2.2.6, as we no longer require $\gcd(i, j) = 1$.

Using Theorem 3.1.6, it is very difficult to find an $a, b \in k$ that work with a given i and j. Instead, given an $a, b \in k$ we will try to find which i, j will make $S(k; i, j, a, b)$ non-trivial.

3.2 Finding $\mathcal{A}_k$ for Minimal Fields

The rest of this chapter will be devoted to analyzing the minimal fields. By Theorem 3.1.7, if $b = 0$, we have that if $S(k; i, j, a, b)$ is not trivial, then $i = j = 1$. Therefore, from now on, we will only consider the situation where $b \neq 0$. If $S(k; i, j, a, b)$ is non-trivial, by Theorem

3.1.9 and Theorem 3.1.3 we have that $g(i+j) = 0$ and so $x^{i+j} = g(i+j)x - bg(i+j-1) \in k$. Also, by Theorem 2.1.8, we have that x^{i+j} is in the center of $S(k; i, j, a, b)$ and so $x^{i+j} \in k$. If r and s are roots of $x^2 - ax + b$ and we consider diagonalizing x, then we are looking for i and j such that $r^{i+j} = s^{i+j}$. If x is not diagonalizable, then x can be put in Jordan normal form and we are looking for i and j that make x^{i+j} a multiple of the identity. It is important to note that the characteristic polynomial for x corresponds to the characteristic polynomial for g.

We begin with a lemma that can be proven using basic difference-equation solution techniques.

Lemma 3.2.1. *Let k be a field, $g : k \to k$ be given by $g(0) = 0$, $g(1) = 1$ and $g(n) = ag(n-1) - bg(n-2)$ for $n \geq 2$, and $x^2 - ax + b$ be the corresponding characteristic polynomial to g.*

(i) Let r and s be distinct roots of $x^2 - ax + b$, then

$$g(n) = \frac{1}{r-s}r^n - \frac{1}{r-s}s^n.$$

(ii) Let r be the repeated root of $x^2 - ax + b$, then

$$g(n) = nr^{n-1}.$$

We will begin the analysis of minimal fields with the field $\mathbb{Q}$. It is important to note that x cannot be a multiple of the identity. If $x^2 - ax + b$ has repeated root r, then the Jordan normal form of x is given by

$$\begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix}.$$

Then

$$x^{i+j} = \begin{pmatrix} r^{i+j} & (i+j)r^{i+j-1} \\ 0 & r^{i+j} \end{pmatrix},$$

which can never be a multiple of the identity unless $r = 0$. This idea is summed up in the following lemma.

Lemma 3.2.2. *If $x^2 - ax + b$ has repeated roots and $b \neq 0$, then $S(\mathbb{Q}; i, j, a, b)$ is trivial.*

Proof. Suppose $x^2 - ax + b$ has repeated root r, then by Lemma 3.2.1 we have $g(n) = nr^{n-1}$ which is never 0 if $n \geq 1$. Therefore, by Theorem 3.1.6, the algebra $S(\mathbb{Q}; i, j, a, b)$ is trivial. □

We will now find allowable roots for $x^2 - ax + b$ so that $S(\mathbb{Q}; i, j, a, b)$ is non-trivial.

Lemma 3.2.3. *Let $p(x) = x^2 - ax + b$ be separable with distinct roots r and s. If $S(\mathbb{Q}; i, j, a, b)$ is non-trivial, then $r, s \in \mathbb{R}$ or s is the complex conjugate of r.*

Proof. Suppose r and s are the distinct roots of $x^2 - ax + b$. Since $p(x) \in \mathbb{Q}[x]$, then $p(r) = 0$ if and only if $0 = \overline{p(r)} = p(\bar{r})$. Hence, either both roots of p are real or $s = \bar{r}$. □

The following theorem will show us for which $a, b \in \mathbb{Q}$ there exist i and j such that $S(\mathbb{Q}; i, j, a, b)$ is non-trivial. We begin with a lemma from Galois theory.

Lemma 3.2.4. *Let $m, n \in \mathbb{N}_0$ such that $n \neq 0$, $\gcd(m, n) = 1$, and $\frac{m}{n} < 1$. Then, $\cos(\frac{m}{n}2\pi) \in \mathbb{Q}$ if and only if*

$$\frac{m}{n}2\pi \in \left\{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}\right\}$$

Proof. Let m and n satisfy the hypotheses above and suppose $\cos(\frac{m}{n}2\pi)$ is rational. The

element $\omega = e^{i\frac{m}{n}2\pi}$ is a primitive n-th root of unity and

$$\cos\left(\frac{m}{n}2\pi\right) = \frac{\omega + \bar{\omega}}{2}.$$

Consider the Galois extension $\mathbb{Q}(\omega)$. Let $\psi : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ be an automorphism that fixes $\mathbb{Q}$, then $\psi(\omega) = \omega^k$ for some $k \in \mathbb{N}$ where $\gcd(k, n) = 1$ since ψ permutes primitive roots of $x^n - 1$. Since ψ fixes $\mathbb{Q}$ we get $\psi\left(\cos(\frac{m}{n}2\pi)\right) = \cos(\frac{m}{n}2\pi)$ and so

$$\begin{aligned}
\cos\left(\frac{m}{n}2\pi\right) &= \psi\left(\cos\left(\frac{m}{n}2\pi\right)\right) \\
&= \psi\left(\frac{\omega + \bar{\omega}}{2}\right) \\
&= \frac{\psi(\omega) + \psi(\bar{\omega})}{2} \\
&= \frac{\omega^k - \bar{\omega}^k}{2} \\
&= \cos\left(\frac{km}{n}2\pi\right).
\end{aligned}$$

Let $0 \leq \frac{k'm}{n} < 1$ such that $\frac{k'm}{n}2\pi = \frac{km}{n}2\pi + 2\pi c$ for $c \in \mathbb{Z}$. For a given $0 \leq \theta < 2\pi$, there are only two angles $0 \leq \rho < 2\pi$ such that $\cos(\rho) = \cos(\theta)$; either $\rho = \theta$ or $\rho = 2\pi - \theta$. Therefore, there are at most two automorphisms on the extension $\mathbb{Q}(\omega)$ that fix $\mathbb{Q}$. Any such automorphism will permute primitive roots of $x^n - 1$, so there must be at most two primitive roots of $x^n - 1$. Therefore, the number of primitive n-th roots of unity is $\phi(n)$, where ϕ is the Euler-ϕ function; the only natural numbers n where $\phi(n) \leq 2$ are 1, 2, 3, 4, and 6. Thus, since $\gcd(m, n) = 1$ and $\frac{m}{n} < 1$, we obtain

$$\begin{aligned}
\frac{m}{n}2\pi &\in \left\{0, \frac{1\cdot 2\pi}{6}, \frac{1\cdot 2\pi}{4}, \frac{1\cdot 2\pi}{3}, \frac{1\cdot 2\pi}{2}, \frac{2\cdot 2\pi}{3}, \frac{3\cdot 2\pi}{4}, \frac{5\cdot 2\pi}{6}\right\} \\
&= \left\{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}\right\}.
\end{aligned}$$

□

Theorem 3.2.5. *If $S(\mathbb{Q}; i, j, a, b)$ is non-trivial, then x^2-ax+b must be one of the following:*

$$x^2 - r^2, x^2 + r^2, x^2 - rx + r^2, x^2 + rx + r^2,$$

$$x^2 - 2rx + 2r^2, x^2 + 2rx + 2r^2, x^2 - 3rx + 3r^2, x^2 + 3rx + 3r^2$$

for some $r \in \mathbb{Q}$.

Proof. Assume $S(k; i, j, a, b)$ is non-trivial. By Theorem 3.2.4 we have that the roots of $x^2 - ax + b$ must either both be real or be conjugates. Assume the roots of $x^2 - ax + b$ are both real and let these roots be r and s. By Lemma 3.2.1, we have

$$g(n) = \frac{1}{r-s}r^n - \frac{1}{r-s}s^n$$

and by Theorem 3.1.9 we have $g(i + j) = 0$, therefore $r^{i+j} = s^{i+j}$. By Lemma 3.2.2, we have that $r \neq s$ and so $s = -r$. Therefore if $x^2 - ax + b$ has real roots, $a = 0$ and $b = -r^2$.

Suppose that $x^2 - ax + b$ has conjugate roots. Again, by Lemma 3.2.2, the roots cannot be the same and thus must not be real. Let λ and $\bar{\lambda}$ be the roots of $x^2 - ax + b$. By Lemma 3.2.1

$$g(n) = \frac{1}{\lambda - \bar{\lambda}}\lambda^n - \frac{1}{\lambda - \bar{\lambda}}\bar{\lambda}^n$$

and, as above $g(i + j) = 0$ and $\lambda^{i+j} = \bar{\lambda}^{i+j}$. Hence we get $|\lambda|^{-2}\lambda^{2(i+j)} = 1$. Lettng $\lambda = se^{\sqrt{-1}\theta}$, we get that $e^{2(i+j)\sqrt{-1}\theta} = 1$ and so $e^{\sqrt{-1}\theta}$ is a root of unity. We also have $a = \lambda + \bar{\lambda} = 2s\cos(\theta)$ and $b = \lambda\bar{\lambda} = s^2$, and so $s^2, s\cos(\theta) \in \mathbb{Q}$, and so $\cos(2\theta) = 2\cos^2(2\theta) - 1 \in \mathbb{Q}$. Since $e^{\sqrt{-1}\theta}$ is a root of unity, $\theta = \frac{m}{n}2\pi$ where $0 \leq m < n$ and

$\gcd(m,n) = 1$, and by Lemma 3.2.4, we get

$$2\theta = 0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}, 2\pi, \frac{7\pi}{3}, \frac{5\pi}{2}, \frac{8\pi}{3}, 3\pi, \frac{10\pi}{3}, \frac{7\pi}{2}, \frac{11\pi}{3}$$

and so,

$$\theta = 0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}, \pi, \frac{7\pi}{6}, \frac{5\pi}{4}, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}, \frac{7\pi}{4}, \frac{11\pi}{6}.$$

With these values for θ, we obtain the polynomials

$$x^2 + s^2, x^2 - sx + s^2, x^2 + sx + s^2, x^2 - \sqrt{2}sx + s^2,$$

$$x^2 + \sqrt{2}sx + s^2, x^2 - \sqrt{3}sx + s^2, x^2 + \sqrt{3}sx + s^2.$$

Since all the coefficients are rational, then $\sqrt{2}s = 2r \in \mathbb{Q}$ and $s^2 = 2r^2$ or $\sqrt{3}s = 3r \in \mathbb{Q}$ and so $s^2 = 3r^2$ with $r \in \mathbb{Q}$ in both cases. Thus, we obtain the rest of the polynomials in the statement of the theorem. □

It should be noted that values found for θ in the previous proof are the exact values we teach students to remember on the unit circle in a trigonometry class. Thus, the cosine (or sine) of a rational multiple of π will be a square-root of a rational number if and only if it is one of the angles found in the proof above. These angles are those of the special right-triangles taught in a beginning trigonometry course.

Theorem 3.2.6. *For $i, j \in \mathbb{N}$, we have $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$ if and only if*

$$(i, j) \equiv (1, 1) \pmod 2,$$

$$(i, j) \equiv (1, 2), (2, 1), (4, 5), (5, 4) \pmod 6,$$

or $(i, j) = (2 + 4n, 2 + 4n)$ for some $n \in \mathbb{N}_0$.

Proof. By Theorem 3.2.5, we have a list of the allowable polynomials that may make $S(\mathbb{Q}; i, j, a, b)$ non-trivial for some i and j. Thus, we only need to analyze the sequences they generate. By Theorem 3.1.7 we have $(1, 1, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$, and so we need only worry when $r \neq 0$.

Case 1) $x^2 - r^2$: Here the sequence g is

$$0, 1, 0, r^2, 0, r^4, \ldots$$

If $r = 1$ or $r = -1$, then if $(i, j) \equiv (1, 1) \pmod 2$, then i and j satisfy the conditions of Theorem 3.1.6, and so $S(\mathbb{Q}; i, j, 0, -1)$ is non-trivial and $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. If $r \neq 1, -1$, then if $i = j$ and i is odd, then $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. This is of course a subset of $(i, j) \equiv (1, 1) \pmod 2$.

Case 2) $x^2 + r^2$: Here the sequence g is

$$0, 1, 0, -r^2, 0, r^4, \ldots$$

If $r = 1$ or $r = -1$, then if $(i, j) \equiv (1, 1), (3, 3) \pmod 4$, then i and j satisfy the conditions of Theorem 3.1.6, and so $S(\mathbb{Q}; i, j, 0, 1)$ is non-trivial and $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. If $r \neq 1, -1$, then if $i = j$ and i is odd, then $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. This is of course a subset of $(i, j) \equiv (1, 1) \pmod 2$.

Case 3) $x^2 - rx + r^2$: Here the sequence g is

$$0, 1, r, 0, -r^3, -r^4, 0, r^5, r^6, \ldots$$

If $r = 1$, then if $(i, j) \equiv (1, 2), (2, 1), (4, 5), (5, 4) \pmod 6$, then i and j satisfy the conditions of Theorem 3.1.6, and so $S(\mathbb{Q}; i, j, 1, 1)$ is non-trivial and $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. There are no i and j that satisfy the conditions of Theorem 3.1.6 if $r \neq 1$.

Case 4) $x^2 + rx + r^2$: Here the sequence g is

$$0, 1, -r, 0, r^3, -r^4, \ldots$$

This case is case (3) if we replace r with $-r$.

Case 5) $x^2 - 2rx + 2r^2$: Here the sequence g is

$$0, 1, 2r, 2r^2, 0, -4r^4, -8r^5, -8r^6, \ldots$$

For any r, if $i = j = 2 + 4n$ for some $n \in \mathbb{N}_0$, then i and j satisfy the conditions of Theorem 3.1.6, and so $S(\mathbb{Q}; i, j, 2r, 2r^2)$ is non-trivial and $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$.

Case 6) $x^2 + 2rx + 2r^2$: Here the sequence g is

$$0, 1, -2r, 2r^2, 0, -4r^4, 8r^5, -8r^6, \ldots$$

This is case (5) if we replace r with $-r$.

Case 7) $x^2 - 3rx + 3r^2$: Here the sequence g is

$$0, 1, 3r, 6r^2, 9r^3, 9r^4, 0, -27r^6, -81r^7, -162r^8, -243r^9, -243r^10, \ldots$$

For any r, if $i = j = 3 + 6n$ for some $n \in \mathbb{N}_0$, then i and j satisfy the conditions of Theorem 3.1.6, and so $S(\mathbb{Q}; i, j, 3r, 3r^2)$ is non-trivial and $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$. This case is a subset of case (1).

Case 8) $x^2 + 3rx + 3r^2$: Here the sequence g is

$$0, 1, 3r, 6r^2, 9r^3, 9r^4, 0, -27r^6, -81r^7, -162r^8, -243r^9, -243r^10, \ldots$$

This case is case (vii) if we replace r with $-r$.

Therefore, $(i, j, 1, 1) \in \mathcal{A}_{\mathbb{Q}}$ if and only if

$$(i, j) \equiv (1, 1) \pmod 2,$$

$$(i, j) \equiv (1, 2), (2, 1), (4, 5), (5, 4) \pmod 6,$$

$$\text{or } (i, j) = (2 + 4n, 2 + 4n) \text{ for some } n \in \mathbb{N}_0.$$

□

We will now consider the minimal finite-fields $\mathbb{F}_p$ for prime p. Let $x^2 - ax + b$ have distinct roots r and s. As stated at the beginning of Section 3.2, we are looking for i and j such that $r^{i+j} = s^{i+j}$. If $x^2 - ax + b$ is reducible, then $r, s \in \mathbb{F}_p$, which is a very difficult question to answer. However, if $x^2 - ax + b$ is irreducible, the roots have a certain symmetry, which we will use to find i and j such that $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial. Note that if $x^2 - ax + b$ is irreducible, then $b \neq 0$. We begin with a lemma about the period of the sequence g.

Lemma 3.2.7. *Let $x^2 - ax + b \in \mathbb{F}_p[x]$ be irreducible with roots $\alpha, \beta \in \mathbb{F}_{p^2}$ and $g : \mathbb{N}_0 \to \mathbb{F}_p$ be the sequence corresponding to the polynomial $x^2 - ax + b$. If d is the order of α and β in the multiplicative group $\mathbb{F}_{p^2} \setminus \{0\}$, then g is has period d.*

Proof. By Lemma 3.2.1, the sequence $g(n)$ has the explicit formula

$$g(n) = \frac{1}{\alpha - \beta}\alpha^n - \frac{1}{\alpha - \beta}\beta^n.$$

Let $c = \alpha - \beta$. Since $|\alpha| = |\beta| = d$, we have $\alpha^d = \beta^d = 1$ and so

$$\begin{aligned} g(n + d) &= \frac{1}{c}\alpha^{n+d} + \frac{1}{c}\beta^{n+d} \\ &= \frac{1}{c}\alpha^n\alpha^d - \frac{1}{c}\beta^n\beta^d \end{aligned}$$

$$= \frac{1}{c}\alpha^n - \frac{1}{c}\beta^n$$

$$= g(n),$$

and thus the period of g is at most d. Suppose g has period k for some $k \leq d$, then $g(k) = g(0) = 0$ and $g(k+1) = g(1) = 1$ and so we have $\frac{1}{c}\alpha^k - \frac{1}{c}\beta^k = 0$ and $\frac{1}{c}\alpha^{k+1} - \frac{1}{c}\beta^{k+1} = 1$. From these equations we get $\alpha^k = \beta^k$ and $\alpha^{k+1} = \beta^{k+1} + \alpha - \beta$. Therefore, $\alpha^{k+1} = \alpha^k\beta + \alpha - \beta$ and so $\alpha^{k+1} - \alpha^k = \alpha - \beta$ and $\alpha^k(\alpha - \beta) = \alpha - \beta$. Since $x^2 - ax + b$ is irreducible over $\mathbb{F}_p$, $\alpha \neq \beta$ and therefore $\alpha^k = 1$. Since $|\alpha| = d$, $k = d$. □

We will first deal with the case where $p = 2$. The polynomial ring $\mathbb{F}_2[x]$ has only one irreducible polynomial: $x^2 + x + 1$. This polynomial generates the sequence $(0, 1, 1, 0, 1, 1, \dots)$, and so $S(\mathbb{F}_2; i, j, 1, 1)$ is non-trivial if and only if $(i, j) \equiv (1, 2), (2, 1) \pmod 3$. We will now consider the case when $p > 2$.

Before moving on we make an important note. The Frobenius map defined as $F(a) = a^p$ is an automorphism on fields of order p^n that fixes the field $\mathbb{F}_p$. The polynomial $x^p - x \in \mathbb{F}_{p^2}$ has exactly p roots, all of which are in $\mathbb{F}_p$. Let a, b, α, and β be defined as in Lemma 3.2.7, then $\mathbb{F}_p[x]/(x^2 - ax + b) \cong \mathbb{F}(\alpha) \cong \mathbb{F}_{p^2}$. Therefore, $F(\alpha) = \alpha^p \neq \alpha$, since $\alpha \notin \mathbb{F}_p$, and thus $F(\alpha) = \beta$ since $\mathbb{F}_p(\alpha)$ is Galois. Similarly $F(\beta) = \alpha$. Therefore, $\alpha^p = \beta$ and $\beta^p = \alpha$ if $x^2 - ax + b$ is irreducible.

Theorem 3.2.8. *Let $p > 2$ and $\bar{a}, \bar{b} \in \mathbb{F}_p$ be such that $x^2 - \bar{a}x + \bar{b}$ be irreducible with roots $\lambda, \psi \in \mathbb{F}_{p^2}$ where λ generates $\mathbb{F}_{p^2} \setminus \{0\}$ as a multiplicative group, then $S(\mathbb{F}_p; i, j, \bar{a}, \bar{b})$ is non-trivial if and only if*

$$(i, j) \equiv \left(n, \frac{p^2 + 2np - 1}{2}\right) \pmod{p^2 - 1} \text{ and } p - 1 \not| n$$

for some $n \geq 1$.

Proof. Let $p > 2$, $\bar{a}, \bar{b} \in \mathbb{F}_p$ and $\lambda, \psi \in \mathbb{F}_{p^2}$ as defined above and let $\bar{g}$ be the sequence corresponding to $x^2 - \bar{a}x + \bar{b}$. Then $\lambda + \psi = \bar{a}$ and $\lambda\psi = \bar{b}$. Since λ (and thus ψ) generate $\mathbb{F}_{p^2} \setminus \{0\}$, then λ and ψ have order $p^2 - 1$. By Lemma 3.2.7, we only need consider i and j modulo $p^2 - 1$. Since $|\lambda| = |\psi| = p^2 - 1$, we have

$$\left|\lambda^{(p^2-1)/2}\right| = \left|\psi^{(p^2-1)/2}\right| = 2$$

and since $\mathbb{F}_{p^2} \setminus \{0\}$ is cyclic of order $p^2 - 1$, the number of elements of order 2 is $\phi(2) = 1$ (where ϕ is the Euler-phi function), thus $\lambda^{(p^2-1)/2} = \psi^{(p^2-1)/2} = -1$. Let $c = \lambda - \psi$. By Lemma 3.2.1, we have

$$\begin{aligned}
\bar{g}\left(\frac{p^2-1}{2}\right) &= \frac{1}{c}\lambda^{(p^2-1)/2} - \frac{1}{c}\psi^{(p^2-1)/2} \\
&= \frac{1}{c}(-1) - \frac{1}{c}(-1) \\
&= 0 \\
&= \bar{g}(0)
\end{aligned}$$

and

$$\begin{aligned}
\bar{b}\bar{g}\left(\frac{p^2-1}{2} - 1\right) &= \bar{b}\left[\frac{1}{c}\lambda^{(p^2-1)/2-1} - \frac{1}{c}\psi^{(p^2-1)/2-1}\right] \\
&= \bar{b}\left[\frac{1}{c}(-\lambda^{-1}) - \frac{1}{c}(-\psi^{-1})\right] \\
&= \bar{b}\left[\frac{1}{c\psi} - \frac{1}{c\lambda}\right] \\
&= \bar{b}\left[\frac{\lambda - \psi}{c\lambda\psi}\right] \\
&= \bar{b}\left[\bar{b}^{-1}\right]
\end{aligned}$$

$$= \bar{g}(1).$$

Hence,

$$\bar{g}\left(\frac{p^2-1}{2}\right) = \bar{g}(0) \text{ and } \bar{b}\bar{g}\left(\frac{p^2-1}{2}-1\right) = \bar{g}(1). \tag{3.2}$$

Suppose $\bar{g}(i) = \bar{g}(j)$ and $\bar{g}(i+1) = \bar{b}\bar{g}(j-1)$, then

$$\begin{aligned}
\bar{g}(j+p) &= \frac{1}{c}\lambda^{j+p} - \frac{1}{c}\psi^{j+p} \\
&= \frac{1}{c}\left(\lambda^p\lambda^j - \psi^p\psi^j\right) \\
&= \frac{1}{c}\left(\psi\lambda^j - \lambda\psi^j\right) \\
&= \frac{1}{c}\lambda\psi\left(\lambda^{j-1} - \psi^{j-1}\right) \\
&= \bar{b}\left[\frac{1}{c}\lambda^{j-1} - \frac{1}{c}\psi^{j-1}\right] \\
&= \bar{b}\bar{g}(j-1) \\
&= \bar{g}(i+1)
\end{aligned}$$

and, by Lemma 3.1.8 we obtain

$$\begin{aligned}
\bar{b}\bar{g}(j+p-1) &= \bar{b}\left[\frac{1}{c}\lambda^{j+p-1} - \frac{1}{c}\psi^{j+p-1}\right] \\
&= \bar{b}\left[\frac{1}{c}\left(\lambda^p\lambda^{j-1} - \psi^p\psi^{j-1}\right)\right] \\
&= \bar{b}\left[\frac{1}{c}\left(\psi\lambda^{j-1} - \lambda\psi^{j-1}\right)\right] \\
&= \bar{b}\left[\frac{1}{c}\lambda\psi\left(\lambda^{j-2} - \psi^{j-2}\right)\right]
\end{aligned}$$

$$= \bar{b}^2 \left[\frac{1}{c}\lambda^{j-2} - \frac{1}{c}\psi^{j-2} \right]$$

$$= \bar{b}^2 \bar{g}(j-2)$$

$$= \bar{g}(i+2).$$

Therefore $\bar{g}(i+1) = \bar{g}(j+p)$ and $\bar{g}(i+2) = \bar{b}\bar{g}(j+p-1)$. This result along with (3.2) gives

$$\bar{g}(n) = \bar{g}\left(\frac{p^2-1}{2} + np\right) \text{ and } \bar{g}(n+1) = \bar{b}\bar{g}\left(\frac{p^2-1}{2} + np - 1\right)$$

for $n \geq 1$, where the arguments of $\bar{g}$ are taken modulo p^2-1. These relations satisfy two of the conditions of Theorem 3.1.6 for $S(\mathbb{F}_p; i, j, \bar{a}, \bar{b})$ to be non-trivial. Suppose $\bar{g}(k) = 0$. Since $\lambda^2 - a\lambda + b = 0$, by Lemma 3.1.3, $\lambda^k = \bar{g}(k)\lambda - \bar{b}\bar{g}(k-1) = -\bar{b}\bar{g}(k-1) \in \mathbb{F}_p \setminus \{0\}$ and $\lambda^k \in \mathbb{F}_p \setminus \{0\}$, then $\left(\lambda^k\right)^{p-1} = 1$. Since the order of λ is p^2-1, $k(p-1) = m(p^2-1) = m(p+1)(p-1)$. Therefore, $k = m(p+1)$ for some $m \in \mathbb{N}_0$. Let $m \in \mathbb{N}_0$, then

$$\bar{g}(m(p+1)) = \frac{1}{c}\lambda^{m(p+1)} - \frac{1}{c}\psi^{m(p+1)}$$

$$= \frac{1}{c}\left((\lambda^p)^m\lambda^m - (\psi^p)^m\psi^m\right)$$

$$= \frac{1}{c}\left(\psi^m\lambda^m - \lambda^m\psi^m\right)$$

$$= 0$$

and so $\bar{g}(k) = 0$ if and only if k is a multiple of $p+1$. Therefore, if

$$(i,j) \equiv \left(n, \frac{p^2+2np-1}{2}\right) \pmod{p^2-1} \text{ and } p-1 \nmid n$$

for some $n \geq 1$, then $S(\mathbb{F}_p; i, j, \bar{a}, \bar{b})$ is non-trivial.

Suppose there is some $j \not\equiv (p^2 + 2np - 1)/2 \pmod{p^2 - 1}$ with $0 \leq j < p^2 - 1$ such that $S(\mathbb{F}_p; n, j, \bar{a}, \bar{b})$ is non trivial. Let $k = (p^2 + 2np - 1)/2 \pmod{p^2 - 1}$, then

$$\bar{g}(n) = \bar{g}(j) = \bar{g}(k) \text{ and } \bar{g}(n+1) = \bar{b}\bar{g}(j-1) = \bar{b}\bar{g}(k-1),$$

so $\bar{g}(j-1) = \bar{g}(k-1)$ and $\bar{g}(j) = \bar{g}(k)$ where $0 \leq j, k < p^2 - 1$. However, since two consecutive terms define this second-order recursive sequence and the period of $\bar{g}$ is $p^2 - 1$, this is a contradiction since $j \neq k$. Therefore, if $S(\mathbb{F}_p; i, j, \bar{a}, \bar{b})$ is non-trivial, then

$$(i, j) \equiv \left(n, \frac{p^2 + 2np - 1}{2}\right) \pmod{p^2 - 1} \text{ and } p - 1 \not| n.$$

□

It is important to note, since $\mathbb{F}_{p^2} \setminus \{0\}$ is cyclic, if $x^2 - ax + b \in \mathbb{F}_p[x]$ is irreducible, then the sequence it generates is a rescaled subsequence of $\bar{g}$. This leads us to the following theorem.

Theorem 3.2.9. *Let $p > 2$, $\bar{a}, \bar{b} \in \mathbb{F}_p$, $\lambda, \psi \in \mathbb{F}_{p^2}$, and $\bar{g}$ be defined as in Theorem 3.2.8. If $x^2 - ax + b \in \mathbb{F}_p[x]$ is irreducible with roots α and β, then $\alpha = \lambda^k$ and $\beta = \psi^k$ for some $0 \leq k < p^2 - 1$ and $S(\mathbb{F}_p; i, j, a, b)$ is no-trivial if and only if $S(\mathbb{F}_p; ki, kj, \bar{a}, \bar{b})$ is non-trivial.*

Proof. Suppose $p > 2$ and $x^2 - ax + b$ is irreducible with roots α and β and let $\bar{a}, \bar{b} \in \mathbb{F}_p$, $\lambda, \psi \in \mathbb{F}_{p^2}$, and $\bar{g}$ be defined as above. Since λ generates $\mathbb{F}_{p^2} \setminus \{0\}$ multiplicatively, then there exists $0 \leq k < p^2 - 1$ such that $\alpha = \lambda^k$, and since the Frobenius map permutes roots of irreducible polynomials in $\mathbb{F}_p[x]$,

$$\beta = \alpha^p = (\lambda^k)^p = (\lambda^p)^k = \psi^k,$$

and

$$b = \alpha\beta = \lambda^k\psi^k = (\lambda\psi)^k = \bar{b}^k.$$

Suppose $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial and let g be the sequence generated by $x^2 - ax + b$, then $g(i) = g(j)$, $g(i+1) = b(j-1)$, and $g(j) \neq 0$. Let $c = \alpha - \beta$, then from the equation $g(i) = g(j)$ and by Lemma 3.2.1 we have

$$\frac{1}{c}(\alpha^i - \beta^i) = \frac{1}{c}(\alpha^j - \beta^j)$$

and so $\lambda^{ki} - \psi^{ki} = \lambda^{kj} - \psi^{kj}$ and $\bar{g}(ki) = \bar{g}(kj)$. From $g(i+1) = bg(j-1)$ we obtain,

$$\frac{1}{c}(\alpha^{i+1} - \beta^{i+1}) = b\frac{1}{c}(\alpha^{j-1} - \beta^{j-1}))$$

so

$$\begin{aligned}(\lambda^k)^{i+1} - (\psi^k)^{i+1} &= b^k((\lambda^k)^{j-1} - (\psi^k)^{j-1})\lambda^{ki+k} - \psi^{ki+k} \\ &= b^k(\lambda^{jk-k} - \psi^{jk-k})\end{aligned}$$

and $\bar{g}(ki+k) = \bar{b}^k\bar{g}(jk-k)$ and by repeated use of Lemma 3.1.8, $\bar{g}(ki+1) = \bar{b}\bar{g}(jk-1)$. Finally, since $g(j) \neq 0$ and

$$g(j) = \frac{1}{c}\alpha^j - \frac{1}{c}\beta^j,$$

we have $\alpha^j \neq \beta^j$ and so $\lambda^{jk} \neq \psi^{jk}$ and so $\bar{g}(jk) \neq 0$. Therefore, $S(\mathbb{F}_p; ki, kj, \bar{a}, \bar{b})$ is non-trivial.

Suppose $S(\mathbb{F}_p; ki, kj, \bar{a}, \bar{b})$ is non-trivial. Then $\bar{g}(ki) = \bar{g}(kj)$, $\bar{g}(ki+1) = \bar{b}\bar{g}(kj-1)$, and $\bar{g}(j) \neq 0$. Again, using Lemma 3.1.8, $g(ki+k) = b^k g(kj-k)$. Following the steps above in reverse, we get that $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial. □

Theorem 3.2.10. *Let $p > 2$, $a, b \in \mathbb{F}_p$ such that $x^2 - ax + b$ is irreducible over $\mathbb{F}_p$ with roots $\alpha, \beta \in \mathbb{F}_{p^2}$ and let $(p^2-1)/d$ be the order of α in $\mathbb{F}_{p^2} \setminus \{0\}$. Then $S(\mathbb{F}_p; i, j, a, b) \cong M_2(\mathbb{F}_p)$ if and only if*

$$(i, j) \equiv \left(\frac{n}{d}, \frac{p^2 + 2np - 1}{2d}\right) \pmod{(p^2-1)/d}$$

for some $n \geq 1$ where $p + 1 \not| n$, $d = \gcd(|\alpha|, p^2 - 1)$, and d divides n and $(p^2 + 2np - 1)/2$.

Proof. Let $p > 2$, $x^2 - ax + b$ be irreducible with roots $\alpha, \beta \in \mathbb{F}_{p^2}$ with $\lambda \in \mathbb{F}_{p^2}$ defined in Theorem 3.2.8. Let $t = |\alpha|$ in the multiplicative group $\mathbb{F}_{p^2} \setminus \{0\}$. Then t divides $p^2 - 1$. Let $d = (p^2 - 1)/t$ and g be the sequence generated by $x^2 - ax + b$, then by Lemma 3.2.7, g has period $t = (p^2 - 1)/d$ and we need only consider $0 \leq i, j < (p^2 - 1)/d$. There exists $0 \leq k < p^2 - 1$ such that $\alpha = \lambda^k$. The order of α is $t = (p^2 - 1)/\gcd(k, p^2 - 1)$, so $\gcd(k, p^2 - 1) = d$ and $k = md$ for some m. By the same argument as in the proof of Theorem 3.2.8, for any given n there is at most one $0 \leq j < (p^2 - 1)/d$ such that $S(\mathbb{F}_p; i, j, a, b)$ non-trivial. Assume $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial. By Theorem 3.2.9, $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial if and only if $S(\mathbb{F}_p; mdi, mdj, \bar{a}, \bar{b})$ is non-trivial. Letting

$$n \equiv mdi \pmod{p^2 - 1} \text{ then } mdj \equiv \frac{p^2 + 2np - 1}{2} \pmod{p^2 - 1}$$

by Theorem 3.2.8. Since d divides mdi, mdj, and $p^2 - 1$, d divides n and $\frac{p^2+2np-1}{2}$. Since mdi and mdj generate the same set as di and dj modulo $p^2 - 1$, we may assume $k = d$. So, $S(\mathbb{F}_p; i, j, a, b) \cong M_2(\mathbb{F}_p)$ if and only if

$$(i, j) \equiv \left(\frac{n}{d}, \frac{p^2 + 2np - 1}{2d}\right) \pmod{(p^2-1)/d}$$

where d divides n, $(p^2 + 2np - 1)/2$, and $p^2 - 1$. □

We now treat the case when $x^2 - ax + b \in \mathbb{F}_p[x]$ is inseparable and thus has a repeated root. This root must be in $\mathbb{F}_p$, since all irreducible polynomials in $\mathbb{F}_p[x]$ are separable. Consider $x^2 - 2rx + r^2$, which has repeated root r. If $S(\mathbb{F}_p; i, j, 2r, r^2)$ is non-trivial, then the image of x will have the Jordan normal form

$$\begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix}.$$

It is both interesting and important to note that

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a, b \in \mathbb{F}_p, a \neq 0 \right\}$$

forms a cyclic group under multiplication with order $p(p-1)$. We will use this structure in a way similar to the the way we used the structure of $\mathbb{F}_{p^2} \setminus \{0\}$, which is also cyclic. We begin with a lemma about the sequence g.

Lemma 3.2.11. *Let $x^2 - ax + b \in \mathbb{F}_p[x]$ have repeated root $r \in \mathbb{F}_p \setminus \{0\}$ and $g : \mathbb{N}_0 \to \mathbb{F}_p$ be the sequence corresponding to the polynomial $x^2 - ax + b$. Let d be the order of r in the multiplicative group $\mathbb{F}_p \setminus \{0\}$, then g has period pd.*

Proof. By Lemma 3.2.1, $g(n)$ has the explicit formula

$$g(n) = nr^{n-1}.$$

Since $|r| = d$ we get

$$\begin{aligned} g(n + pd) &= (n + pd)r^{n+pd-1} \\ &= nr^{n-1}r^{pd} + pdr^{n+pd-1} \end{aligned}$$

$$= nr^{n-1}$$

$$= g(n),$$

and thus the period of g is at most pd. Suppose the period of g is k for some $k \leq d$, then $g(k) = g(0) = 0$ and $g(k+1) = g(1) = 1$ and so we obtain $kr^{k-1} = 0$ and $(k+1)r^k = 1$. Since $kr^{k-1} = 0$ and $r \neq 0$, then $k = mp$ for some $m \in \mathbb{N}_0$. From the equation $(k+1)r^k = 1$ we get $1 = (k+1)r^k = kr^k + r^k = r^k$ and so $k = nd$ for some $n \in \mathbb{N}_0$, since $|r| = d$. Since p is prime, $k = cpd$ for some $c \in \mathbb{N}_0$, but $k \leq pd$ so $k = pd$. Therefore, the period of g is pd. □

We will first deal with the case when $p = 2$. The polynomial ring $\mathbb{F}_2[x]$ has only one polynomial with repeated roots not equal to 0: $x^2 + 1$. This polynomial generates the sequence $(0, 1, 0, 1, 0, 1, \dots)$ and so $S(\mathbb{F}_2; i, j, 0, 1)$ is non-trivial if and only if $(i, j) \equiv (1, 1) \pmod 2$. We will now consider the case when $p > 2$.

Theorem 3.2.12. *Let $p > 2$ and $s \in \mathbb{F}_p \setminus \{0\}$ such that s generates $\mathbb{F}_p \setminus \{0\}$ multiplicatively, then $S(\mathbb{F}_p; i, j, 2s, s^2)$ is non-trivial if and only if*

$$(i, j) \equiv \left(n, \frac{p(p-1) + 2(2p-1)n}{2}\right) \pmod{p(p-1)}$$

for some $n \geq 1$ where $p \not| n$.

Proof. Let $p > 2$ and $s \in \mathbb{F}_p$ be defined as above and let $\bar{g}$ be the sequence generated by $x^2 - 2sx + s^2$. Since s generates $\mathbb{F}_p$, $|s| = p - 1$ and by Lemma 3.2.11, we need only consider i and j modulo $p(p-1)$. Since $|s| = p - 1$, we have

$$|s^{p(p-1)/2}| = |s^p s^{(p-1)2}| = |s^{(p-1)/2}| = 2,$$

and since $\mathbb{F}_p$ is cyclic with only one element of order 2, then $s^{p(p-1)/2} = -1$. By Lemma

3.2.1, we have

$$\begin{aligned}\bar{g}\left(\frac{p(p-1)}{2}\right) &= \frac{p(p-1)}{2}s^{p(p-1)/2-1}\\ &= p\frac{p-1}{2}s^{p(p-1)/2-1}\\ &= 0\\ &= \bar{g}(0)\end{aligned}$$

and

$$\begin{aligned}s^2\bar{g}\left(\frac{p(p-1)}{2}-1\right) &= s^2\left(\frac{p(p-1)}{2}-1\right)s^{p(p-1)/2-1-1}\\ &= s^2p\frac{p-1}{2}s^{p(p-1)/2-2} - s^2s^{p(p-1)/2-2}\\ &= -s^2(-1)s^{-2}\\ &= 1\\ &= \bar{g}(1).\end{aligned}$$

Hence

$$\bar{g}(0) = \bar{g}\left(\frac{p(p-1)}{2}\right) \text{ and } \bar{g}(1) = s^2\bar{g}\left(\frac{p(p-1)}{2}-1\right). \tag{3.3}$$

Suppose $\bar{g}(i) = \bar{g}(j)$ and $\bar{g}(i+1) = s^2\bar{g}(j-1)$, then

$$\begin{aligned}\bar{g}(j+2p-1) &= (j+2p-1)s^{j+2p-1-1}\\ &= (j-1)s^{j-2}s^{2p} + 2ps^{j+2p-2}\\ &= (j-1)s^{j-2}(s^p)^2\end{aligned}$$

$$= s^2\bar{g}(j-1)$$

$$= \bar{g}(i+1)$$

and, by Lemma 3.1.8 we obtain

$$\begin{aligned} s^2\bar{g}(j+2p-2) &= s^2(j+2p-2)s^{j+2p-2-1} \\ &= s^2(j-2)s^{j-3}s^{2p} + 2ps^{j+2p-3} \\ &= s^2(j-2)s^{j-3}(s^p)^2 \\ &= s^4\bar{g}(j-2) \\ &= \bar{g}(i+2). \end{aligned}$$

Therefore, $\bar{g}(i+1) = \bar{g}(j+2p-1)$ and $\bar{g}(i+2) = s^2\bar{g}(j-2)$. This result, along with equation (3.3) gives

$$\bar{g}(n) = \bar{g}\left(\frac{p(p-1)}{2} + n(2p-1)\right) \text{ and } \bar{g}(n+1) = \bar{g}\left(\frac{p(p-1)}{2} + n(2p-1) - 1\right)$$

for $n \geq 1$, where the arguments of $\bar{g}$ are taken modulo $p(p-1)$. Suppose $\bar{g}(k) = 0$, then $0 = ks^{k-1}$. Since $s \neq 0$, this is true if and only if $k = mp$ for some $m \in \mathbb{N}_0$. Therefore, if

$$(i,j) \equiv \left(n, \frac{p(p-1) + 2(2p-1)n}{2}\right) \pmod{p(p-1)}$$

for some $n \geq 1$ where $p \not| n$, then $S(\mathbb{F}_p; i, j, 2s, s^2)$ is non-trivial.

Suppose there is some $j \not\equiv (p(p-1)+2(2p-1)n)/2 \pmod{p(p-1)}$ with $0 \leq j < p(p-1)$ such that $S(\mathbb{F}_p; n, j, 2s, s^2)$ is non trivial. Let $k = (p(p-1)+2(2p-1)n)/2 \pmod{p(p-1)}$.

Then

$$\bar{g}(n) = \bar{g}(j) = \bar{g}(k) \text{ and } \bar{g}(n+1) = s^2\bar{g}(j-1) = s^2\bar{g}(k-1),$$

so $\bar{g}(j-1) = \bar{g}(k-1)$ and $\bar{g}(j) = \bar{g}(k)$ where $0 \leq j, k < p(p-1)$. This is a contradiction since two consecutive terms define this recursive sequence and the period of $\bar{g}$ is $p(p-1)$. Therefore, if $S(\mathbb{F}_p; i, j, 2s, s^2)$ is non-trivial, then

$$(i, j) \equiv \left(n, \frac{p(p-1) + 2(2p-1)n}{2}\right) \pmod{p(p-1)} \text{ and } p \nmid n.$$

□

Since

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a, b \in \mathbb{F}_p, a \neq 0 \right\}$$

is cyclic, if $x^2 - ax + b$ has a repeated root (not 0), then the sequence it generates is a rescaled subsequence of $\bar{g}$, which leads to the following theorem.

Theorem 3.2.13. *Let $p > 2$ and let $s \in \mathbb{F}_p$ generate $\mathbb{F}_p$ multiplicatively as in Theorem 3.2.12. For $r \in \mathbb{F}_p \setminus \{0\}$, $S(\mathbb{F}_p; i, j, 2r, r^2)$ is non-trivial if and only if $S(\mathbb{F}_p; ki, kj, 2r, r^2)$ where $r = s^k$ and $r \neq 1$.*

Proof. Let $p > 2$ and suppose $r = 1$. Then $g(n) = n(1)^{n-1} = n$. The sequence generated by $x^2 - 2x + 1$ is then $(0, 1, 2, 3 \ldots, p-1, 0, 1, 2 \ldots)$. Since $r = 1$, there are no i and j such that $g(i) = g(j)$ and $g(i+1) = r^2 g(j-1) = g(j-1)$. Therefore $S(\mathbb{F}_p; i, j, 2, 1)$ is always trivial.

Let s and $\bar{g}$ be defined as in Theorem 3.2.12 and $r \neq 1$, then there exists $0 < k < p$ such that $r = s^k$. Let g be the sequence generated by the polynomial $x^2 - 2rx + r^2$. Suppose $S(\mathbb{F}_p; i, j, 2r, r^2)$ is non-trivial, then by Theorem 3.1.6 $g(i) = g(j)$, $g(i+1) = r^2 g(j-1)$, and $g(j) \neq 0$. Since $g(i) = g(j)$ we have that $ir^{i-1} = jr^{j-1}$ and since $0 < k < p$, we get

$ki(s^k)^{i-1} = kj(s^k)^{j-1} \neq 0$ and so $kis^{ki-k} = kjs^{kj-k}$ and finally $kis^{ki-1} = kjs^{kj-1}$. Hence $\bar{g}(ki) = \bar{g}(kj)$ and $\bar{g}(j) \neq 0$. From the equation $g(i+1) = r^2 g(j-1)$ we obtain $(i+1)r^i = r^2(j-1)r^{j-2}$. We have $k(i+1)(s^k)^i = (s^k)^2 k(j-1)(s^k)^{j-2}$ and so $(ki+k)s^{ki} = (s^2)^k(kj-k)s^{kj-2k}$ and finally, $(ki+k)s^{ki+k-1} = (s^2)^k s^{kj-k-1}$. Therefore, $\bar{g}(ki+k) = (s^2)^k \bar{g}(kj-k)$ and so by Lemma 3.1.8, we get $\bar{g}(ki+1) = s^2\bar{g}(kj-1)$. Hence, $S(\mathbb{F}_p; ki, kj, 2s, s^2)$ is non-trivial.

Suppose $S(\mathbb{F}_p; ki, kj, 2s, s^2)$ is non-trivial. Then $\bar{g}(ki) = \bar{g}(kj)$, $\bar{g}(ki+1) = s^2\bar{g}(kj-1)$, and $\bar{g}(j) \neq 0$. Again, using Lemma 3.1.8, $g(ki+k) = (s^2)^k g(kj-k)$. Following the steps above in reverse, we get that $S(\mathbb{F}_p; i, j, 2r, r^2)$ is non-trivial. □

Theorem 3.2.14. *Let $a, b \in \mathbb{F}_p$ such that $x^2 - ax + b$ has a repeated root $r \in \mathbb{F}_p$ that is not 0 and let $(p-1)/d$ be the order of r in $\mathbb{F}_p \setminus \{0\}$. Then $S(\mathbb{F}_p; i, j, a, b) \cong M_2(\mathbb{F}_p)$ if and only if*

$$(i, j) \equiv \left(\frac{n}{d}, \frac{p(p-1) + 2(2p-1)n}{2d}\right) \pmod{(p(p-1))/d}$$

for some $n \geq 1$ where $p \not| n$, d divides n, and $(p(p-1) + 2(2p-1)n)/2$.

Proof. Let $p > 2$, $r \in \mathbb{F}_p \setminus \{0\}$ with $s \in \mathbb{F}_p$ defined as in Theorem 3.2.12. Let $t = |r|$ in the multiplicative group $\mathbb{F}_p \setminus \{0\}$. Then t divides $p-1$. Let $d = (p-1)/t$ and g be the sequence generated by $x^2 - ax + b$, then by Lemma 3.2.11, g has period $tp = (p(p-1))/d$ and we need only consider $0 \leq i, j < (p(p-1))/d$. There exists $0 \leq k < p-1$ such that $r = s^k$. If $k = 0$, then $r = 1$ and by Theorem 3.2.13, $S(\mathbb{F}_p; i, j, a, b)$ is trivial. Suppose $k \neq 0$. The order of r is $t = (p-1)/\gcd(k, p-1)$, so $\gcd(k, p-1) = d$ and $k = md$ for some m. By the same argument as in the proof of Theorem 3.2.12, there is at most one $0 \leq j < (p(p-1))/d$ that will make $S(\mathbb{F}_p; i, j, a, b)$ non-trivial. Assume $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial. By Theorem 3.2.13, $S(\mathbb{F}_p; i, j, a, b)$ is non-trivial if and only if $S(\mathbb{F}_p; mdi, mdj, 2s, s^2)$

is non-trivial. Letting

$$n \equiv mdi \pmod{p(p-1)} \text{ then } mdj \equiv \frac{p^2+2np-1}{2} \pmod{(p(p-1))}$$

by Theorem 3.2.8. Since d divides mdi, mdj, and $p-1$, we have d divides n and $\frac{p^2+2np-1}{2}$. Since mdi and mdj generate the same set as di and dj modulo p^2-1, we may assume $k = d$. Note if $r = 1$, then $d = p-1$ and if $p-1|n$, then $p-1 \not|((p(p-1)/2 + (2p-1)n)$. So, $S(\mathbb{F}_p; i, j, a, b) \cong M_2(\mathbb{F}_p)$ if and only if if

$$(i,j) \equiv \left(\frac{n}{d}, \frac{p(p-1)+2(2p-1)n}{2d}\right) \pmod{(p(p-1))/d}$$

for some $n \geq 1$ where $p \not| n$, d divides n, and $(p(p-1)+2(2p-1)n)/2$. □

The following corollary to Theorem 3.2.10 and Theorem 3.2.14 gives a collection of many of the elements of $\mathcal{A}_{\mathbb{F}_p}$.

Corollary 3.2.15. *If*

$$(i,j) \equiv \left(\frac{n}{d}, \frac{p^2+2np-1}{2d}\right) \pmod{(p^2-1)/d}$$

for some $n \geq 1$ where $p+1 \not| n$, $d = \gcd(|\alpha|, p^2-1)$, and d divides n and $(p^2+2np-1)/2$ or

$$(i,j) \equiv \left(\frac{n}{d}, \frac{p(p-1)+2(2p-1)n}{2d}\right) \pmod{(p(p-1))/d}$$

for some $n \geq 1$ where $p \not| n$, d divides n, and $(p(p-1)+2(2p-1)n)/2$, then $(i,j,1,1) \in \mathcal{A}_{\mathbb{F}_p}$.

Unfortunately, the sequences generated by reducible, separable polynomials do not have a structure as nice as those sequences generated by inseparable or irreducible polynomials over $\mathbb{F}_p$. However, we are still able to directly compute for which $(i,j,1,1) \in \mathcal{A}_{\mathbb{F}_p}$, since

there are only finitely many polynomials in $\mathbb{F}_p[x]$ and the sequences they generate are all periodic. For example $(i,j,1,1) \in \mathcal{A}_{\mathbb{F}_2}$ if and only if $(i,j) \equiv (1,1) \pmod 2$ or $(i,j) \equiv (1,2),(2,1) \pmod 3$ and $(i,j,1,1) \in \mathcal{A}_{\mathbb{F}_3}$ if and only if $(i,j) \equiv (1,1) \pmod 2$, $(i,j) \equiv (1,2),(2,1),(4,5),(5,4) \pmod 6$, or $(i,j) \equiv (1,7),(2,2),(3,5),(5,3),(6,6),(7,1) \pmod 9$. Corollary 3.2.15 gives us many of these (i,j), the rest can be computed simply by direct computation of the sequences generated by separable, reducible polynomials.

3.3 Further Questions

There are many interesting questions that result from this research.

First, we have seen that not all $R(A;i,j,1,1)$ are complete matrix rings as seen in Example 2.3.4. However, we showed that $R(\mathbb{F}_2;2,2,1,1)$ can be embedded in a matrix ring over a commutative ring. Can all $R(A;i,j,1,1)$, or more generally, $R(A;i,j,m,n)$ be embedded in a matrix ring over a commutative ring?

Second, as asked at the end of Section 3.2, for which i and j is $S(\mathbb{F}_p;i,j,a,b)$ non-trivial when $x^2 - ax + b$ is reducible and separable?

Next, by using the structure of irreducible polynomials and inseparable polynomials over a finite field, can the results of Theorem 3.2.10 and Theorem 3.2.14 be extended to the fields $\mathbb{F}_{p^n}$ for any $n > 1$?

Finally, by Theorem 1.3 of [**?**] we have a set of matrix units for $R(A;i,j,m,n)$. Using these matrix units, is there a description for $R(A;i,j,m,n)$ similar to the description for $R(A;i,j,1,1)$ from Theorem 2.2.6 when $\gcd(i,j) = 1$?

Curriculum Vitae

Sam Mendelson graduated from Phoenix Country Day School in 2004. He received his Bachelor of Science in Mathematics from George Washington University in 2008. He received his Master of Science in Mathematics from George Mason University in 2012.