PRODUCTS OF INVOLUTIONS OVER FIELDS

by

Christina T. Tsiaparas–Plazomites

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in the

Mathematics

Program

YOUNGSTOWN STATE UNIVERSITY

December, 1996

Products Of Involutions Over Fields

Christina T. Tsiaparas–Plazomites

I hereby release this thesis to the public. I understand this thesis will be housed at the Circulation Desk of the University library and will be available for public access. I also authorize the University or other individuals to make copies of this thesis as needed for scholarly research.

Signature:

C. T. Tsiaparas Plazomites December 6, 1996

Student Date

Approvals:

F. A. Arlinghaus December 6, 1996

Thesis Advisor Date

S. F. Barger December 6, 1996

Committee Member Date

A. C. Burns 6 Dec 1996

Committee Member Date

Peter J. Kasvinsky December 10, 1996

Dean of Graduate Studies Date

Abstract

We consider matrices in the group $\pm SL(n, F)$ of all invertible $n \times n$ matrices of determinant ± 1 with entries over the field F that can be written as the product of involutions, and we show that any such matrix can be written as the product of at most four involutions. We also consider special cases of matrices in this group that can be written as the product of exactly two or three involutions, and we show how this concept of factoring a matrix into a product of involutions can be extended to special classes of rings that are not fields.

Contents

Section 1. Introduction

There are many important and well-known theorems in mathematics that deal with the factorization of objects into products of special types. For example, the Fundamental Theorem of Arithmetic states that every positive integer can be factored uniquely, up to order, as a product of prime numbers, and a similar theorem in algebra states that any polynomial over a field can be factored uniquely, up to order and constant factors, as the product of irreducible polynomials over the field. Other examples of the same theme include that any permutation of a finite set of at least two elements can be factored as a product of transpositions, that any $n \times n$ positive definite matrix can be factored as the product of a lower triangular and upper triangular matrix, that any $n \times n$ matrix can be factored as the product of at most n reflections, and that any invertible matrix can be factored as the product of elementary matrices.

The problem that we are examining is another type of special factorization of a matrix, this time as product of involutions, i.e., matrices that are their own inverses. The question that is to be answered is as follows:

> *Does there exist a smallest positive integer k, such that for any matrix $A \in \pm SL(n, F)$ which is a product of involutions, A can be written as the product of at most k involutions, and, if such an integer exists, what is it?*

(Note: $\pm SL(n, F)$ is the group of all invertible $n \times n$ matrices of determinant ± 1 over the field F.)

We will begin our examination of the factorization of matrices as the product of involutions by first stating precise definitions of basic terms that are to be used in the remainder of the paper. These definitions, along with examples, are given in Section 2, so the reader might want to skip this section and refer back to it as needed. Some more introductory material is presented in Section 3, which, as a foundation for the following sections, contains a general discussion of involutions, their determinants, and how they relate to the groups $GL(n, F)$ and $\pm SL(n, F)$.

The main discussion of the problem that we are trying to solve begins in Section 4 and continues in Sections 5 and 6. In Section 4 the special case of matrices that can be written as the product of two involutions is examined, examples of such matrices are presented, and related theorems are stated and proven.

Section 5 contains examples of matrices that cannot be written as the product of two or three involutions, and so the number of involutions needed in such a product must be greater than or equal to four, and the main theorem of this paper, the Four Involutions Theorem, which proves that four involutions suffice in every case, is stated and proven.

Following the main theorem of Section 5, Section 6 deals with special cases of matrices that can be written as a product of exactly three involutions, and again examples are given and related theorems are stated and proven. In Section 7 we discuss how we can generalize this concept of factoring a matrix as a product of special matrices if we pass to rings of special types which are not fields, and we look at what has to be true of these rings, and of what form these special matrices must be. Finally, Section 8 contains a summary of the problem discussed in this paper and of the various results that were presented, and it is mentioned how this concept of factoring matrices into special products can be extended to other classes of matrices.

Section 2. Definitions and Examples

Definition 1. *(Involutory Matrices) Let F be any field and consider the general linear group $GL(n, F)$ of all invertible $n \times n$ matrices with entries over F, and let $A \in GL(n, F)$ such that $A^2 = I_n$. Then A is called an involutory matrix, or, more simply, an involution.* $\diamond$

Example 1. *(2 × 2 Involutory Matrix)*

Consider the matrix $Y = \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix} \in GL(2, Z_{11})$. Since

$$Y^2 = \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix}\begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix} = \begin{bmatrix} 34 & 22 \\ 99 & 67 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2,$$

it follows that Y is an *involution*. $\diamond$

Example 2. *(3 × 3 Involutory Matrix)*

Consider the matrix $A = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} \in GL(3, Z_7)$. Since

$$A^2 = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix}\begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4+0-3 & -2-1+3 & -6+0+6 \\ 0+0+0 & 0+1+0 & 0+0+0 \\ 2+0-2 & -1-1+2 & -3+0+4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

it follows that A is an *involution*. $\diamond$

Definition 2. *(Similar Matrices) Two matrices A and B in $M(n, F)$, the group of all $n \times n$ matrices over a field F, are similar if there exists an invertible matrix $X \in GL(n, F)$, such that $A = X^{-1}BX$.* $\diamond$

Example 3. *(Similar Matrices in Z_{11})*

Consider the matrices $A = \begin{bmatrix} 5 & 8 \\ 5 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 5 \\ 4 & 2 \end{bmatrix}$ both in $M(2, Z_{11})$. Then A and B are *similar* since there exists an invertible matrix $X = \begin{bmatrix} 1 & 2 \\ 4 & 7 \end{bmatrix} \in GL(2, Z_{11})$, with $X^{-1} = \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix}$, such that

$$X^{-1}BX = \begin{bmatrix} 4 & 2 \\ 4 & 10 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 4 & 2 \end{bmatrix}X = \begin{bmatrix} 8 & 2 \\ 10 & 7 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 16 & 30 \\ 38 & 69 \end{bmatrix} = \begin{bmatrix} 5 & 8 \\ 5 & 3 \end{bmatrix} = A. \quad \diamond$$

Example 4. *(Similar Matrices in Z_5)*

Consider the matrices $A = \begin{bmatrix} 2 & 0 \\ 4 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 2 \\ 4 & 0 \end{bmatrix}$ both in $M(2, Z_5)$. Then A and B are *similar* since there exists an invertible matrix $X = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \in GL(2, Z_5)$, with $X^{-1} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$, such that

$$X^{-1}BX = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 4 & 0 \end{bmatrix}X = \begin{bmatrix} 1 & 1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ 4 & 11 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 4 & 1 \end{bmatrix} = A. \quad \diamond$$

Note 1.

Let $A \in M(n, F)$ and $D \in M(n, F)$ be similar matrices. So there exists some matrix $B \in GL(n, F)$, such that $B^{-1}AB = D$. Now if A is non-singular then we have

$$D = B^{-1}AB \Rightarrow \det(D) = \det(B^{-1})\det(A)\det(B) \neq 0,$$

and so it follows that D is also non-singular. $\diamond$

Definition 3. *(Involutorily Similar Matrices) Two matrices A and B in $M(n, F)$ are involutorily similar if they are similar, and an involution is implementing the similarity (i.e., there exists some involution $X \in GL(n, F)$, such that $A = X^{-1}BX$).* $\diamond$

Example 5. *(Involutorily Similar Matrices)*

Consider the matrices $A = \begin{bmatrix} 7 & 5 \\ 6 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 3 \\ 5 & 2 \end{bmatrix}$, and $X = \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix}$ which are all in $GL(2, Z_{11})$.

By Example 1, X is an involution, and since

$$X^{-1}BX = XBX = \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 5 & 2 \end{bmatrix}X = \begin{bmatrix} 7 & 5 \\ 0 & 8 \end{bmatrix}\begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix} = \begin{bmatrix} 73 & 49 \\ 72 & 56 \end{bmatrix} = \begin{bmatrix} 7 & 5 \\ 6 & 1 \end{bmatrix} = A,$$

it follows that A and B are *involutorily similar*. $\diamond$

Definition 4. *(Adjoint of a Matrix) The adjoint, denoted by $adj(A)$ or by A^*, of a matrix $A \in M(n, F)$, is the transpose of the matrix with elements γ_{ij}, where $i, j = 1, 2, 3, \ldots, n$, and $\gamma_{ij} = (-1)^{i+j}\det(A_{ij})$.* $\diamond$

Example 6. *(Adjoint of a Matrix)*

Consider the matrix $A = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 7 & 2 \\ 1 & 3 & 0 \end{bmatrix} \in M(3, \mathbf{R})$.

Then

$$\gamma_{11} = (-1)^2 \det\begin{bmatrix} 7 & 2 \\ 3 & 0 \end{bmatrix} = -6, \quad \gamma_{12} = (-1)^3 \det\begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix} = 2, \quad \gamma_{13} = (-1)^4 \det\begin{bmatrix} 3 & 7 \\ 1 & 3 \end{bmatrix} = 2,$$

$$\gamma_{21} = (-1)^3 \det\begin{bmatrix} 2 & 5 \\ 3 & 0 \end{bmatrix} = 15, \quad \gamma_{22} = (-1)^4 \det\begin{bmatrix} 1 & 5 \\ 1 & 0 \end{bmatrix} = -5, \quad \gamma_{23} = (-1)^5 \det\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = -1,$$

$$\gamma_{31} = (-1)^4 \det\begin{bmatrix} 2 & 5 \\ 7 & 2 \end{bmatrix} = -31, \quad \gamma_{32} = (-1)^5 \det\begin{bmatrix} 1 & 5 \\ 3 & 2 \end{bmatrix} = 13, \text{ and } \gamma_{33} = (-1)^6 \det\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} = 1.$$

$$\text{So, } \Gamma = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} \end{bmatrix} = \begin{bmatrix} -6 & 2 & 2 \\ 15 & -5 & -1 \\ -31 & 13 & 1 \end{bmatrix}, \text{ therefore } adj(A) = \Gamma^T = \begin{bmatrix} -6 & 15 & -31 \\ 2 & -5 & 13 \\ 2 & -1 & 1 \end{bmatrix}. \quad \diamond$$

Definition 5. *(Unitary Matrix) A matrix $A \in M(n, F)$, is said to be unitary if $A^*A = I_n$, where A^* is the adjoint of A if $F \neq \mathbf{C}$, and A^* is the transposed conjugate $(\overline{A})^T$ of A if $F = \mathbf{C}$.* $\diamond$

Example 7. *(2 × 2 Unitary Matrix)*

Let $K = \begin{bmatrix} 2 & 7 \\ 1 & 4 \end{bmatrix} \in M(2, \mathbf{R})$.

Then $\Gamma = \begin{bmatrix} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{bmatrix} = \begin{bmatrix} 4 & -1 \\ -7 & 2 \end{bmatrix}$, so $K^* = adj(K) = \Gamma^T = \begin{bmatrix} 4 & -7 \\ -1 & 2 \end{bmatrix}$.

Now

$$K^*K = \begin{bmatrix} 4 & -7 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 7 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 8-7 & 28-28 \\ -2+2 & -7+8 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2.$$

Hence, K is a *unitary* 2×2 *matrix*. $\diamond$

Example 8. *(3 × 3 Unitary Matrix)*

Consider the matrix $A = \frac{1}{3}\begin{bmatrix} -2 & 2 & -1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{bmatrix} \in M(3, \mathbf{R})$.

Then $\Gamma = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} \end{bmatrix} = \frac{1}{3}\begin{bmatrix} -2 & 2 & -1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{bmatrix}$, so $A^* = adj(A) = \Gamma^T = \frac{1}{3}\begin{bmatrix} -2 & 1 & 2 \\ 2 & 2 & 1 \\ -1 & 2 & -2 \end{bmatrix}$.

Now

$$A^*A = \frac{1}{3}\begin{bmatrix} -2 & 1 & 2 \\ 2 & 2 & 1 \\ -1 & 2 & -2 \end{bmatrix} \frac{1}{3}\begin{bmatrix} -2 & 2 & -1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{bmatrix} = \frac{1}{9}\begin{bmatrix} 4+1+4 & -4+2+2 & 2+2-4 \\ -4+2+2 & 4+4+1 & -2+4+-2 \\ 2+2-4 & -2+4+-2 & 1+4+4 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3.$$

Hence it follows that A is a *unitary* 3×3 *matrix*. $\diamond$

Definition 6. *(Unitary Involution) A matrix $A \in M(n, F)$, is said to be a unitary involution if both of the following hold:*

1) A is unitary (i.e., $A^*A = I_n$), and

2) A is an involution (i.e., $AA = I_n$),

or, in other words, A is a *unitary involution* if $A^* = A = A^{-1}$. $\diamond$

Example 9. *(2 × 2 Unitary Involution)*

Consider the matrix $X = \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix} \in M(2, Z_{11})$ from Example 1. Now X is an involution (as shown in Example 1) and also $X^* = adj(X) = \begin{bmatrix} 7 & -2 \\ -9 & 4 \end{bmatrix}$, and so it follows that

$$X^*X = adj(X)X = \begin{bmatrix} 7 & -2 \\ -9 & 4 \end{bmatrix} \begin{bmatrix} 4 & 2 \\ 9 & 7 \end{bmatrix} = \begin{bmatrix} 10 & 0 \\ 0 & 10 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I_2.$$

Since $X^*X \neq I_2$, then X is not a *unitary involution*, and so not all involutions are unitary involutions. $\diamond$

Example 10. (3 × 3 Unitary Involution)

Let $A = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} \in M(3, Z_7)$. Then we know from Example 2 that A is an involution.

Now $A^* = adj(A) = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} = A$, and so $A^*A = adj(A)A = AA = I_3$, so it follows that A is a *unitary involution.* $\diamond$

Definition 7. (Unimodular Matrix) *Let $A \in GL(n, F)$. Then if $\det(A) = 1$, or $\det(A) = -1$, A is said to be a unimodular matrix (i.e., if $A \in \pm SL(n, F)$, A is said to be unimodular).* $\diamond$

Example 11. (Unimodular Matrix)

Let $A = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \in GL(3, Z_3)$.

Then

$$\det(A) = -1 \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = -1(1-2) = -1(-1) = 1,$$

and so it follows that A is *unimodular* (i.e., $A \in \pm SL(3, Z_3)$). $\diamond$

Definition 8. (Characteristic Polynomial) *Let $A \in M(n, R)$, the group of all $n \times n$ matrices with entries over a ring R. The characteristic polynomial of A, denoted be $C_A(x)$, is defined by*

$$C_A(x) = \det(A - xI_n),$$

where $C_A(x)$ is of the form

$$C_A(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0. \quad \diamond$$

Example 12. (Characteristic Polynomial)

Let $A \in M(2, Z_5)$ be defined by $A = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$.

Then

$$C_A(x) = \det\left(\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix} - x\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \det\begin{bmatrix} 2-x & 1 \\ 4 & 3-x \end{bmatrix} = (2-x)(3-x) - 4 = x^2 - 5x + 6 - 4 = x^2 + 2,$$

is the *characteristic polynomial* of A. $\diamond$

Note 2.

Since $C_A(x)$ is of the form

$$C_A(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0,$$

for any $A \in M(n, R)$, it follows that $C_A(x) \in R[x]$, the ring of all polynomials in the indeterminate x with coefficients in R.

Also, every monic polynomial of degree n in $R[x]$ is the characteristic polynomial of some $n \times n$ matrix in $M(n, R)$, as will be seen in the following definition. $\diamond$

Definition 9. *(Companion Matrix) Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$ be a monic polynomial in $R[x]$, where R is a ring, with $deg(f) \geq 1$. Define the $n \times n$ matrix $Com(f) \in M(n, R)$ by*

$$Com(f) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Then

$$\det[xI_n - Com(f)] = det \begin{bmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & x & a_{n-2} \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix} = f(x),$$

and $Com(f)$ is said to be the *companion matrix* of the monic polynomial $f(x)$. If $deg(f) = 0$, then $Com(f)$ does not exist. $\diamond$

Note 3.

The characteristic polynomial $C_{Com(f)}$ of the companion matrix of $f(x)$ is given by

$$C_{Com(f)}(x) = \det[Com(f) - xI_n] = \det[-I_n(xI_n - Com(f))] = \det(-I_n)\det(xI_n - Com(f)) = (-1)^n f(x).$$

Since the characteristic polynomial $Com(f)$, of the companion matrix of $f(x)$, is $(-1)^n f(x)$, then every polynomial of degree n in $R[x]$ with leading coefficient $(-1)^n$ is the characteristic polynomial of some matrix in $M(n, R)$. $\diamond$

Example 13. *(Companion Matrix)*

Let $f(x) = x^3 + 5x^2 + 3x + 4 \in Z_7[x]$. Then the *companion matrix* of $f(x)$ is the 3×3 matrix in $M(3, Z_7)$ defined by

$$Com(f) = \begin{bmatrix} 0 & 0 & -4 \\ 1 & 0 & -3 \\ 0 & 1 & -5 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 3 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{bmatrix}.$$

Note that

$$C_{Com(f)}(x) = \det[Com(f) - xI_n] = \det\left(\begin{bmatrix} 0 & 0 & 3 \\ 1 & 0 & 4 \\ 0 & 1 & 2 \end{bmatrix} - \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{bmatrix}\right) = \det \begin{bmatrix} -x & 0 & 3 \\ 1 & -x & 4 \\ 0 & 1 & 2-x \end{bmatrix} =$$

$$-x\begin{vmatrix} -x & 4 \\ 1 & 2-x \end{vmatrix} - \begin{vmatrix} 0 & 3 \\ 1 & 2-x \end{vmatrix} = -x(-2x + x^2 - 4) - (-3) = -x^3 + 2x^2 + 4x + 3 =$$

$$-(x^3 - 2x^2 - 4x - 3) = -(x^3 + 5x^2 + 3x + 4) = (-1)^3 f(x). \diamond$$

Definition 10. *(Cyclic Matrix) A cyclic matrix is a matrix that is similar to the companion matrix of an irreducible polynomial.* ◇

Example 14. *(Cyclic Matrix)*

Let $f(x) = x^3 + 2x + 1 \in Z_7[x]$. Then, since $f(x)$ has no zeros in Z_7, it follows that $f(x)$ is irreducible over Z_7, and also the companion matrix $Com(f) \in M(3, Z_7)$ of $f(x)$ is defined by

$$Com(f) = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix}.$$

Now let the matrix $A \in M(3, Z_7)$ be defined by $A = \begin{bmatrix} -2 & 0 & -3 \\ 0 & 2 & -2 \\ -2 & -1 & 0 \end{bmatrix}$. Then there exists a matrix $B = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ -1 & -1 & -2 \end{bmatrix} \in GL(3, Z_7)$, with $B^{-1} = \begin{bmatrix} -2 & -1 & -2 \\ -3 & 1 & 3 \\ -1 & 0 & -1 \end{bmatrix}$, such that $B^{-1}AB =$ $\begin{bmatrix} -2 & -1 & -2 \\ -3 & 1 & 3 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} -2 & 0 & -3 \\ 0 & 2 & -2 \\ -2 & -1 & 0 \end{bmatrix} B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ -3 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ -1 & -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} = Com(f).$

Therefore we have shown that A is similar to the companion matrix of an irreducible polynomial, and so it follows that A is *cyclic.* ◇

Definition 11. *(Block Submatrix) Given an $m \times n$ matrix A with entries over a ring R, if a number of complete rows or columns of A are deleted, or if some complete rows and complete columns of A are deleted, the new matrix that is obtained is called a block submatrix of A.* ◇

Example 15. *(Block Submatrix)*

Let $A = \begin{bmatrix} 2 & 3 & 5 & 6 \\ 7 & 8 & 9 & 10 \\ 1 & 2 & 8 & 12 \end{bmatrix} \in M(3 \times 4, \mathbf{R})$.

Then $B = \begin{bmatrix} 3 & 5 \\ 8 & 9 \end{bmatrix}, C = [5], D = [2 \quad 3 \quad 5 \quad 6]$, are some of the *block submatrices* of A. ◇

Definition 12. *(Block Matrix) A block matrix $A \in M(m \times n, R)$, where R is a ring, is a matrix of the form*

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mn} \end{bmatrix}$$

with block submatrices A_{ij} of A, where A_{ij} is an $M_i \times N_j$ matrix. ◇

Example 16. *(Block Matrix)*

Let $A = \begin{bmatrix} 1 & 2 & 3 & 4 & 1 & 1 \\ 18 & 7 & 5 & 9 & 8 & 2 \\ 5 & 7 & 11 & 0 & 1 & 4 \end{bmatrix} \in M(3 \times 6, \mathbf{R})$.

Define A_{11}, A_{12}, A_{13}, A_{21}, A_{22}, A_{23} as follows:

$$A_{11} = \begin{bmatrix} 1 & 2 \\ 18 & 7 \end{bmatrix} \in M(2 \times 2, \mathbf{R}), \quad A_{12} = \begin{bmatrix} 3 & 4 & 1 \\ 5 & 9 & 8 \end{bmatrix} \in M(2 \times 3, \mathbf{R}),$$

$$A_{13} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \in M(2 \times 1, \mathbf{R}), \quad A_{21} = [5 \quad 7] \in M(1 \times 2, \mathbf{R}),$$

$$A_{22} = [11 \quad 0 \quad 1] \in M(1 \times 3, \mathbf{R}), \quad A_{23} = [4] \in M(1 \times 1, \mathbf{R}).$$

Then $M_1 = 2, M_2 = 1$, and $N_1 = 2, N_2 = 3, N_3 = 1$, and also each A_{ij} is a block submatrix of A, and so it follows that

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{bmatrix}$$

is a *block matrix*. $\diamond$.

Definition 13. (Block Diagonal or Quasidiagonal Matrix) *The matrix A is block diagonal or quasidiagonal, if it has the partitioned form*

$$A = \begin{bmatrix} A_{11} & 0 & \cdots & 0 \\ 0 & A_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{pp} \end{bmatrix},$$

where the matrices A_{ii} are all square matrices but not necessarily of the same size.

Sometimes the notation $diag(A_{11}, A_{22}, \ldots, A_{pp})$, is used to denote a *block diagonal matrix*. $\diamond$

Example 17. (Block Diagonal or Quasidiagonal Matrix)

$$\text{Let } A = \begin{bmatrix} 5 & 7 & 0 & 0 & 0 & 0 \\ 3 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 9 & 9 \\ 0 & 0 & 0 & 2 & 7 & 20 \\ 0 & 0 & 0 & 3 & 12 & 6 \end{bmatrix} \in M(6, \mathbf{R}).$$

Then A is a *block diagonal* or *quasidiagonal matrix* composed of the blocks $A_{11} = \begin{bmatrix} 5 & 7 \\ 3 & 11 \end{bmatrix}$, which is a 2×2 block, $A_{22} = [4]$, which is a 1×1 block, and $A_{11} = \begin{bmatrix} 1 & 9 & 8 \\ 2 & 7 & 20 \\ 3 & 12 & 6 \end{bmatrix}$, which is a 3×3 block. $\diamond$

Note 4.

Let $D = diag(D_1, D_2, \ldots, D_n)$ be a block diagonal matrix in $GL(n, R)$, where R is a ring. Then D^{-1} exists, and is defined by

$$D^{-1} = diag(D_1^{-1}, D_2^{-1}, \ldots, D_n^{-1}).$$

For example, consider the block diagonal matrix $D = diag(D_1, D_2) \in GL(6, \mathbf{R})$, defined by

$$D = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & -2 & 2 \end{bmatrix} = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix}.$$

Then $D_1 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix}$, and $D_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & -2 & 0 \\ 1 & -2 & 2 \end{bmatrix}$.

Now both D_1 and D_2 are non-singular, with $D_1^{-1} = \begin{bmatrix} 1 & -1/2 & 0 \\ 0 & 1/2 & -1/3 \\ 0 & 0 & 1/3 \end{bmatrix}$, and $D_2^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 1/2 & -1/2 & 0 \\ 0 & -1/2 & 1/2 \end{bmatrix}$, and so it follows that

$$D^{-1} = diag(D_1^{-1}, D_2^{-1}) = \begin{bmatrix} 1 & -1/2 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & -1/3 & 0 & 0 & 0 \\ 0 & 0 & 1/3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & -1/2 & 0 \\ 0 & 0 & 0 & 0 & -1/2 & 1/2 \end{bmatrix} = \begin{bmatrix} D_1^{-1} & 0 \\ 0 & D_2^{-1} \end{bmatrix}.$$

To verify that $D^{-1} = diag(D_1^{-1}, D_2^{-1})$, as defined, is indeed that inverse of $D = diag(D_1, D_2)$, we can quickly compute that

$$DD^{-1} = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix} \begin{bmatrix} D_1^{-1} & 0 \\ 0 & D_2^{-1} \end{bmatrix} = \begin{bmatrix} D_1 D_1^{-1} & 0 \\ 0 & D_2 D_2^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ and that}$$

$$D^{-1}D = \begin{bmatrix} D_1^{-1} & 0 \\ 0 & D_2^{-1} \end{bmatrix} \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix} = \begin{bmatrix} D_1^{-1} D_1 & 0 \\ 0 & D_2^{-1} D_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad \diamond$$

Definition 14. *(<u>Direct Sum of Matrices</u>) The direct sum of n matrices, $M_1, M_2, \ldots, M_n$, in this order, is the matrix M of the form*

$$M = \begin{bmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_n \end{bmatrix},$$

denoted by

$$M = M_1 \oplus M_2 \oplus M_3 \oplus \cdots \oplus M_n,$$

where the main diagonal of each M_i lies on the main diagonal of M. $\diamond$

Example 18. *(Direct Sum of Matrices)*

Let $A = \begin{bmatrix} 2 & -1 \\ -4 & 2 \end{bmatrix} \in M(2 \times 2, \mathbf{R})$, and $B = \begin{bmatrix} 3 & 1 & 5 \\ 0 & 2 & 9 \end{bmatrix} \in M(2 \times 3, \mathbf{R})$. Then

$$A \oplus B = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 \\ -4 & 2 & 0 & 0 & 0 \\ 0 & 0 & 3 & 1 & 5 \\ 0 & 0 & 0 & 2 & 9 \end{bmatrix} \in M(4 \times 5, \mathbf{R}),$$

is the *direct sum* of the matrices A and B. $\diamond$

Definition 15. *(Diagonalizable Matrix) A matrix $A \in M(n, R)$, where R is a ring, is said to be diagonalizable, if there exists a matrix $B \in GL(n, R)$, such that $B^{-1}AB = C$, where C is a diagonal matrix (i.e., $C = (c_{ij})$ is an $n \times n$ matrix with $c_{ij} = 0$, for all $i \neq j$).* $\diamond$

Example 19. *(Diagonalizable Matrix)*

Let $A = \begin{bmatrix} -19 & 6 \\ -35 & 10 \end{bmatrix} \in M(2, \mathbf{R})$. Then since there exists a matrix $B = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \in GL(2, \mathbf{R})$, with $B^{-1} = \begin{bmatrix} 5 & -2 \\ -7 & 3 \end{bmatrix}$, such that

$$B^{-1}AB = \begin{bmatrix} 5 & -2 \\ -7 & 3 \end{bmatrix} \begin{bmatrix} -19 & 6 \\ -35 & 10 \end{bmatrix} B = \begin{bmatrix} -25 & 10 \\ 28 & -12 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} = \begin{bmatrix} -5 & 0 \\ 0 & -4 \end{bmatrix} = C,$$

where $C \in M(2, \mathbf{R})$ is a diagonal matrix, it follows that A is a *diagonalizable matrix*. ◇

Definition 16. *(Block Decomposable Matrix) A matrix $A \in M(n, F)$, where F is a field, is said to be block decomposable if it is similar to a block diagonal matrix, $diag(A_{11}, A_{22})$, of more than one block, where $A_{11} \in M(n_1, F)$, $A_{22} \in M(n_2, F)$, and $n_1, n_2 > 0$, with $n_1 + n_2 = n$.*

Otherwise the matrix A is said to be *block indecomposable*. ◇

Example 20. *(Block Decomposable Matrix)*

Let $A = \begin{bmatrix} 1 & 5 & 5 \\ 3 & 2 & 1 \\ 5 & 0 & 1 \end{bmatrix} \in M(3, \mathbf{R})$. Then since there exists a matrix $B = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & -1 \\ 3 & 1 & 1 \end{bmatrix} \in GL(3, \mathbf{R})$, with $B^{-1} = \frac{1}{8} \begin{bmatrix} -2 & 2 & 2 \\ 5 & -1 & -1 \\ 1 & -5 & 3 \end{bmatrix}$, such that

$$B^{-1}AB = \frac{1}{8} \begin{bmatrix} -2 & 2 & 2 \\ 5 & -1 & -1 \\ 1 & -5 & 3 \end{bmatrix} \begin{bmatrix} 1 & 5 & 5 \\ 3 & 2 & 1 \\ 5 & 0 & 1 \end{bmatrix} B = \frac{1}{8} \begin{bmatrix} 14 & -6 & -6 \\ -3 & 23 & 23 \\ 1 & -5 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & -1 \\ 3 & 1 & 1 \end{bmatrix} = \frac{1}{8} \begin{bmatrix} -16 & 16 & 0 \\ 112 & 40 & 0 \\ 0 & 0 & 8 \end{bmatrix} =$$

$$\begin{bmatrix} -2 & 2 & 0 \\ 14 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix} = C,$$

where $C = diag(C_{11}, C_{22}) \in M(3, \mathbf{R})$ is a block diagonal matrix with blocks $C_{11} = \begin{bmatrix} -2 & 2 \\ 14 & 5 \end{bmatrix} \in M(2, \mathbf{R})$, and $C_{22} = [\,1\,] \in M(1, \mathbf{R})$, it follows that A is a *block decomposable matrix*. ◇

Example 21. *(Block Indecomposable Matrix)*

Consider the matrix $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \in M(2, \mathbf{R})$ (note that A is a *Jordan canonical matrix* as defined in Definition 17). Then if A is block decomposable, it follows that there exists some non-singular matrix $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2, \mathbf{R})$, with $B^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in GL(2, \mathbf{R})$, such that

$$B^{-1}AB = P,$$

where $P \in M(2, \mathbf{R})$ is a block diagonal matrix of the form $P = \begin{bmatrix} p_{11} & 0 \\ 0 & p_{22} \end{bmatrix}$.

So we have

$$B^{-1}AB = \tfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} B = \tfrac{1}{ad-bc}\begin{bmatrix} 2d & d-2b \\ -2c & -c+2a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} =$$

$$\tfrac{1}{ad-bc}\begin{bmatrix} 2ad+cd-2bc & d^2 \\ -c^2 & 2ad-cd-2bc \end{bmatrix} = \begin{bmatrix} p_{11} & 0 \\ 0 & p_{22} \end{bmatrix},$$

which means that the following equations must both hold:

$$\frac{1}{ad-bc}(d^2) = 0 \Rightarrow d^2 = 0 \Rightarrow d = 0, \text{ and}$$
$$\frac{1}{ad-bc}(-c^2) = 0 \Rightarrow -c^2 = 0 \Rightarrow c = 0.$$

However, since $d = c = 0$, then $ad - bc = 0$, so B is singular, and so we have a contradiction. So it follows that there can not exist any matrix $B \in GL(2, \mathbf{R})$, such that $B^{-1}AB = P$, where P is a block diagonal matrix of more than one block, and so, by Definition 16, A is *block indecomposable.* ◇

Note 5.

If two block diagonal matrices are similar, and their blocks are block indecomposable, then their blocks are similar in pairs.

For example the block diagonal matrices C and D, both in $M(3, \mathbf{R})$, defined by $C = \begin{bmatrix} 6 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 6 \end{bmatrix}$, and $D = \begin{bmatrix} 10 & -2 & 0 \\ 8 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix}$ are similar since there exists a matrix $B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} \in GL(3, \mathbf{R})$, with

$$B^{-1} = \begin{bmatrix} 1 & -1/2 & 0 \\ 0 & 1/2 & -1/3 \\ 0 & 0 & 1/3 \end{bmatrix}, \text{ such that}$$

$$B^{-1}DB = \begin{bmatrix} 1 & -1/2 & 0 \\ 0 & 1/2 & -1/3 \\ 0 & 0 & 1/3 \end{bmatrix}\begin{bmatrix} 10 & -2 & 0 \\ 8 & 2 & 0 \\ 0 & 0 & 6 \end{bmatrix} B = \begin{bmatrix} 6 & -3 & 0 \\ 4 & 1 & 2 \\ 0 & 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 6 & 0 & 0 \\ 4 & 6 & 0 \\ 0 & 0 & 6 \end{bmatrix} = C.$$

Now the blocks of D are $D_1 = \begin{bmatrix} 10 & -2 \\ 8 & 2 \end{bmatrix}$, which can be shown to be block indecomposable just as we did for the matrix in Example 21, and $D_2 = [6]$, which is clearly block indecomposable, and the blocks of C are $C_1 = \begin{bmatrix} 6 & 0 \\ 4 & 6 \end{bmatrix}$, which can be shown to be block indecomposable, and $C_2 = [6]$, which is block indecomposable. Clearly D_2 is similar to C_2, since they are equal, and so it follows that D_1 must be similar to C_1. This is easy to verify, since there exists a matrix $K = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \in GL(2, \mathbf{R})$, with $K^{-1} = \begin{bmatrix} 1 & -1/2 \\ 0 & 1/2 \end{bmatrix}$, such that

$$K^{-1}D_1K = \frac{1}{2}\begin{bmatrix} 2 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 10 & -2 \\ 8 & 2 \end{bmatrix} K = \frac{1}{2}\begin{bmatrix} 12 & -6 \\ 8 & 2 \end{bmatrix} K = \begin{bmatrix} 6 & -3 \\ 4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 0 \\ 4 & 6 \end{bmatrix} = C_1,$$

and so D is indeed similar to C by blocks. ◇

Note 6.

If every block of a block diagonal matrix $M \in M(n, F)$ can be written as the product of two involutions in $\pm\, SL(n, F)$, then so can the matrix M.

For example consider the block diagonal matrix $M \in M(n,F)$ defined by

$$M = \begin{bmatrix} A_1B_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2B_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_kB_k \end{bmatrix},$$

where each A_i and each B_i are involutions, and let

$$A = \begin{bmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_k \end{bmatrix}, \text{ and } B = \begin{bmatrix} B_1 & 0 & 0 & \cdots & 0 \\ 0 & B_2 & 0 & \cdots & 0 \\ 0 & 0 & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_k \end{bmatrix},$$

where $A, B \in M(n,F)$.

Then we have

$$A^2 = \begin{bmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_k \end{bmatrix} \begin{bmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_k \end{bmatrix} =$$

$$\begin{bmatrix} {A_1}^2 & 0 & 0 & \cdots & 0 \\ 0 & {A_2}^2 & 0 & \cdots & 0 \\ 0 & 0 & {A_3}^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & {A_k}^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} = I_n,$$

and

$$B^2 = \begin{bmatrix} B_1 & 0 & 0 & \cdots & 0 \\ 0 & B_2 & 0 & \cdots & 0 \\ 0 & 0 & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_k \end{bmatrix} \begin{bmatrix} B_1 & 0 & 0 & \cdots & 0 \\ 0 & B_2 & 0 & \cdots & 0 \\ 0 & 0 & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_k \end{bmatrix} =$$

$$\begin{bmatrix} {B_1}^2 & 0 & 0 & \cdots & 0 \\ 0 & {B_2}^2 & 0 & \cdots & 0 \\ 0 & 0 & {B_3}^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & {B_k}^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} = I_n,$$

and so both A and B are involutions.

Now

$$AB = \begin{bmatrix} A_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_k \end{bmatrix} \begin{bmatrix} B_1 & 0 & 0 & \cdots & 0 \\ 0 & B_2 & 0 & \cdots & 0 \\ 0 & 0 & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & B_k \end{bmatrix} = \begin{bmatrix} A_1B_1 & 0 & 0 & \cdots & 0 \\ 0 & A_2B_2 & 0 & \cdots & 0 \\ 0 & 0 & A_3B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & A_kB_k \end{bmatrix} = M,$$

and so it follows that the block diagonal matrix M can be written as the product of two involutions. ◇

Definition 17. *(Jordan Canonical Matrix) A Jordan canonical matrix is an $n \times n$ matrix*

$$\begin{bmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & b_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & a_n \end{bmatrix},$$

such that for each $s = 1, 2, 3, \ldots, n-1$, either $b_s = 0$, or $b_s = 1$ and $a_{s+1} = a_s$. ◇

Example 22. (3 × 3 Jordan Canonical Matrices)

The following are all possible examples of a 3×3 *Jordan canonical matrix* $J \in M(3, F)$:

(a) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$, for any $a \in F$, where a is an eigenvalue with multiplicity 3. Here the Jordan blocks (see Definition 18) are $J_1 = [\,a\,]$, $J_2 = [\,a\,]$, and $J_3 = [\,a\,]$.

(b) $J = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$, for any $a \in F$, where a is an eigenvalue with multiplicity 3. Here the Jordan blocks are $J_1 = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, and $J_2 = [\,a\,]$.

(c) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$, for any $a \in F$, where a is an eigenvalue with multiplicity 3. Here the Jordan blocks are $J_1 = [\,a\,]$, and $J_2 = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$.

(d) $J = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$, for any $a \in F$, where a is an eigenvalue with multiplicity 3. Here the whole matrix is a Jordan block.

(e) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{bmatrix}$, for any $a, b \in F$, $a \neq b$, where a is an eigenvalue with multiplicity 2 and b is an eigenvalue with multiplicity 1. Here the Jordan blocks are $J_1 = [\,a\,]$, $J_2 = [\,a\,]$, and $J_3 = [\,b\,]$.

(f) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{bmatrix}$, for any $a, b \in F$, $a \neq b$, where a is an eigenvalue with multiplicity 2 and b is an eigenvalue with multiplicity 1. Here the Jordan blocks are $J_1 = [\,a\,]$, $J_2 = [\,b\,]$, and $J_3 = [\,a\,]$.

(g) $J = \begin{bmatrix} b & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix}$, for any $a, b \in F$, $a \neq b$, where a is an eigenvalue with multiplicity 2 and b is an eigenvalue with multiplicity 1. Here the Jordan blocks are $J_1 = [\,b\,]$, $J_2 = [\,a\,]$, and $J_3 = [\,a\,]$.

(h) $J = \begin{bmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{bmatrix}$, for any $a, b \in F$, $a \neq b$, where a is an eigenvalue with multiplicity 2 and b is an eigenvalue with multiplicity 1. Here the Jordan blocks are $J_1 = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$, and $J_2 = [\,b\,]$.

(i) $J = \begin{bmatrix} b & 0 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{bmatrix}$, for any $a, b \in F$, $a \neq b$, where a is an eigenvalue with multiplicity 2 and b is an eigenvalue with multiplicity 1. Here the Jordan blocks are $J_1 = [\,b\,]$, and $J_2 = \begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$.

(j) $J = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}$, for any $a, b, c \in F$, $a \neq b \neq c \neq a$, where a, b and c are all eigenvalues with multiplicity 1. Here the Jordan blocks are $J_1 = [\,a\,]$, $J_2 = [\,b\,]$, and $J_3 = [\,c\,]$. $\diamond$

Definition 18. *(<u>Jordan</u> <u>Canonical</u> <u>Form</u> <u>of</u> <u>a</u> <u>Matrix</u>) Any matrix $A \in M(n, R)$, where R is a ring, is similar to a block diagonal matrix of the form*

$$J = diag(J_1, J_2, \ldots, J_p),$$

where each J_i is an $r_i \times r_i$ matrix of the form

$$J_i = \begin{bmatrix} \lambda_i & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_i \end{bmatrix},$$

where each λ_i is an eigenvalue of A and $\sum\limits_{i=1}^{p} r_i = n$.

The matrix J is called the *Jordan canonical form* of A, and the $r_i \times r_i$ matrices J_i are called *Jordan blocks*. $\diamond$

Example 23. *(<u>Jordan</u> <u>Canonical</u> <u>Form</u> <u>of</u> <u>a</u> <u>Matrix</u>)*

The following are examples of the possible *Jordan canonical forms* of a matrix $A \in (4, \mathbf{R})$ with an eigenvalue 2 of multiplicity 4:

(a) $J = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks (see Definition 18) are $J_1 = [\,2\,]$, $J_2 = [\,2\,]$, $J_3 = [\,2\,]$, and $J_4 = [\,2\,]$.

(b) $J = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = [\,2\,]$, $J_2 = [\,2\,]$, and $J_3 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

(c) $J = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = [\,2\,]$, $J_2 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, and $J_3 = [\,2\,]$.

(d) $J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, $J_2 = [\,2\,]$, and $J_3 = [\,2\,]$.

(e) $J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, and $J_2 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

(f) $J = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = [2]$, and $J_2 = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$.

(g) $J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the Jordan blocks are $J_1 = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$, and $J_2 = [2]$.

(h) $J = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$. Here the whole matrix is a Jordan block. ◇

Example 24. *(Jordan Canonical Form of a Matrix)*

Let $A = \begin{bmatrix} 3 & 2 & 1 \\ -1 & 3 & 2 \\ 1 & -3 & -2 \end{bmatrix} \in M(3, \mathbf{R})$. Then

$$\det(A - \lambda I_3) = \begin{vmatrix} 3-\lambda & 2 & 1 \\ -1 & 3-\lambda & 2 \\ 1 & -3 & -2-\lambda \end{vmatrix} = \begin{vmatrix} 3-\lambda & 2 & 1 \\ 0 & -\lambda & -\lambda \\ 1 & -3 & -2-\lambda \end{vmatrix} = (3-\lambda)\begin{vmatrix} -\lambda & -\lambda \\ -3 & -2-\lambda \end{vmatrix} + \begin{vmatrix} 2 & 1 \\ -\lambda & -\lambda \end{vmatrix} =$$

$$(3-\lambda)(2\lambda + \lambda^2 - 3\lambda) + (-2\lambda + \lambda) = -\lambda^3 + 4\lambda^2 - 4\lambda = -\lambda(\lambda^2 - 4\lambda + 4) = -\lambda(\lambda - 2)^2,$$

and so

$\lambda_1 = 0$ is an eigenvalue of A with multiplicity 1, and

$\lambda_2 = 2$ is an eigenvalue of A with multiplicity 2.

Now a linearly independent eigenvector of A (with respect the other eigenvectors of A) associated with the eigenvalue $\lambda_1 = 0$, is $X_1 = \begin{pmatrix} 1 \\ -7 \\ 11 \end{pmatrix}$, since

$$(A - \lambda_1 I_3)X_1 = 0 \Rightarrow (A - 0I_3)X_1 = 0 \Rightarrow \begin{bmatrix} 3 & 2 & 1 \\ -1 & 3 & 2 \\ 1 & -3 & -2 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \text{ and}$$

$$\left[\begin{array}{ccc|c} 3 & 2 & 1 & 0 \\ -1 & 3 & 2 & 0 \\ 1 & -3 & -2 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & -3 & -2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 11 & 7 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & -3 & -2 & 0 \\ 0 & 1 & 7/11 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 0 & -1/11 & 0 \\ 0 & 1 & 7/11 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Now for $\lambda_2 = 2$, since it has multiplicity 2, we must first find a linearly independent eigenvector of A associated with λ_2, and then we must also find a generalized eigenvector of order 2 associated with λ_2.

A linearly independent eigenvector of A (with respect the other eigenvectors of A) associated with the eigenvalue $\lambda_2 = 2$, is $X_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$, since

$$(A - \lambda_2 I_3)X_2 = 0 \Rightarrow (A - 2I_3)X_2 = 0 \Rightarrow \begin{bmatrix} 1 & 2 & 1 \\ -1 & 1 & 2 \\ 1 & -3 & -4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \text{ and}$$

$$\left[\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ -1 & 1 & 2 & 0 \\ 1 & -3 & -4 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 3 & 3 & 0 \\ 0 & -5 & -5 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

A generalized eigenvector of A of order 2 associated with the eigenvalue $\lambda_2 = 2$, is $X_3 = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$, since

$$(A - \lambda_2 I_3)X_3 = X_2 \Rightarrow (A - 2I_3)X_3 = X_2 \Rightarrow \begin{bmatrix} 1 & 2 & 1 \\ -1 & 1 & 2 \\ 1 & -3 & -4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}, \text{ and}$$

$$\left[\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ -1 & 1 & 2 & -1 \\ 1 & -3 & -4 & 1 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 3 & 3 & 0 \\ 0 & -5 & -5 & 0 \end{array}\right] \Rightarrow \left[\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right] = \left[\begin{array}{ccc|c} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Now consider the matrix $P \in M(3, \mathbf{R})$, where

$$P = [X_1 \,|\, X_2 \,|\, X_3] = \begin{bmatrix} 1 & 1 & 2 \\ -7 & -1 & -1 \\ 11 & 1 & 1 \end{bmatrix}.$$

Since the columns of P are linearly independent, then P is non-singular, and we have $P^{-1} = \frac{1}{4}\begin{bmatrix} 0 & 1 & 1 \\ -4 & -21 & -13 \\ 4 & 10 & 6 \end{bmatrix}$.

So it follows that the *Jordan canonical form* J of the 3×3 matrix A is given by

$$J = P^{-1}AP = \frac{1}{4}\begin{bmatrix} 0 & 1 & 1 \\ -4 & -21 & -13 \\ 4 & 10 & 6 \end{bmatrix} \begin{bmatrix} 3 & 2 & 1 \\ -1 & 3 & 2 \\ 1 & -3 & -2 \end{bmatrix} P =$$

$$\begin{bmatrix} 0 & 0 & 0 \\ -1 & -8 & -5 \\ 2 & 5 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 2 \\ -7 & -1 & -1 \\ 11 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix},$$

where the *Jordan blocks* are $J_1 = [\,0\,]$, and $J_2 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$ (so $J = diag(J_1, J_2)$). $\diamond$

Definition 19. *(Matrix Polynomial) An $m \times n$ matrix polynomial, $P(x)$, over a field F, is a matrix whose entries are polynomials with coefficients in F. Such a polynomial can be written either in the form*

$$P(x) = \begin{bmatrix} p_{11}(x) & p_{12}(x) & \cdots & p_{1n}(x) \\ p_{21}(x) & p_{22}(x) & \cdots & p_{2n}(x) \\ \vdots & \vdots & \ddots & \vdots \\ p_{m1}(x) & p_{m2}(x) & \cdots & p_{mn}(x) \end{bmatrix},$$

or, by grouping like powers of the invariant x, in the form

$$P(x) = x^d P_d + x^{d-1} P_{d-1} + \cdots + xP_1 + P_0,$$

where $P_0, P_1, \ldots, P_{d-1}, P_d \in M(m \times n, F)$.

An $n \times n$ square matrix polynomial $P(x)$ is called *invertible* if there is a matrix polynomial $Q(x)$ such that $P(x)Q(x) = I_n$. $\diamond$

Example 25. *(Matrix Polynomial of Degree 3)*

The matrix $P(x) \in M(3, Z_7[x])$, defined by

$$P(x) = \begin{bmatrix} 3x+2 & -3x^3+x^2+2x+1 & -2 \\ 3 & -2x^3+2x & x^2+1 \\ x^2-3x+2 & 2x+3 & -x^2+3 \end{bmatrix},$$

or equivalently by

$$P(x) = x^3 \begin{bmatrix} 0 & -3 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{bmatrix} + x^2 \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{bmatrix} + x \begin{bmatrix} 3 & 2 & 0 \\ 0 & 2 & 0 \\ -3 & 2 & 0 \end{bmatrix} + \begin{bmatrix} 2 & 1 & -2 \\ 3 & 0 & 1 \\ 2 & 3 & 3 \end{bmatrix},$$

is a 3×3 *matrix polynomial.* $\diamond$

Note 7.

The elementary row and column operations on a matrix polynomial over the field F, are defined as follows:

(1) Multiply any row or column by a non-zero $c \in F$,

(2) Interchange any two rows or columns, and

(3) Add to any row (column) any other row (column) multiplied by an arbitrary polynomial $a(x) \in F[x]$. $\diamond$

Definition 20. *(Canonical Matrix Polynomial) An $n \times n$ matrix polynomial $A(x)$ over a field F is equivalent to a diagonal matrix polynomial $A_0(x)$, called a canonical matrix polynomial, where $A_0(x)$ is defined by*

$$A_0(x) = diag[a_1(x), a_2(x), a_3(x), \ldots, a_n(x)],$$

in which for each i, $a_i(x)$ is zero or a monic polynomial, and $a_i(x)$ is divisible by $a_{i-1}(x)$, for $i = 2, 3, \ldots, n$.

Usually $A_0(x)$ is of the form

$$A_0(x) = diag[1, 1, \ldots, 1, a_1(x), a_2(x), \ldots, a_k(x), 0, 0, \ldots, 0],$$

where $a_i(x)$ is a monic polynomial of degree at least 1, and is divisible, for $i = 2, 3, \ldots, k$, by $a_{i-1}(x)$, but it is also possible that the diagonal of $A_0(x)$ contains no zeros or ones. $\diamond$

Definition 21. *(<u>Elementary Divisors</u>) Let $A(x) \in M(n, F[x])$ be a canonical matrix polynomial. Then $A(x)$ has the form*

$$A(x) = diag[a_1(x), a_2(x), a_3(x), \ldots, a_n(x)],$$

where $a_{i-1}(x) \mid a_i(x)$, for $i = 2, 3, \ldots, n,$. The polynomials a_i, for $i = 1, 2, 3, \ldots, n$, are called the elementary divisors of the matrix polynomial $A(x)$. ◇

Example 26. (<u>Canonical 3×3 Matrix Polynomial and Elementary Divisors</u>)

Let $A = \begin{bmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{bmatrix} \in M(3, \mathbf{R})$.

Then, if we use the elementary row operations defined above, the matrix polynomial $A(x) = A - xI_3 \in M(3, l\mathbf{R}[x])$, becomes

$$A(x) = A - xI_3 = \begin{bmatrix} -1-x & -2 & 6 \\ -1 & -x & 3 \\ -1 & -1 & 4-x \end{bmatrix} \Rightarrow \begin{bmatrix} -(x+1) & -2 & 6 \\ -1 & -x & 3 \\ 1 & 1 & x-4 \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} 1 & 1 & x-4 \\ -1 & -x & 3 \\ -(x+1) & -2 & 6 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 1 & x-4 \\ 0 & -x+1 & 3+x-4 \\ 0 & x+1-2 & 6+(x-4)(x+1) \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 1 & x-4 \\ 0 & -(x-1) & x-1 \\ 0 & x-1 & (x-1)(x-2) \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} 1 & 1-1 & (x-4)-(x-4) \\ 0 & -(x-1)-0 & x-1-0 \\ 0 & x-1-0 & (x-1)(x-2)-0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & -(x-1) & x-1 \\ 0 & x-1 & (x-1)(x-2) \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -(x-1) & x-1 \\ 0 & (x-1)-(x-1) & (x-1)(x-2)+(x-1) \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & -(x-1) & x-1 \\ 0 & 0 & (x-1)^2 \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0-0 \\ 0 & -(x-1) & (x-1)-(x-1) \\ 0 & 0 & (x-1)^2+0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & 0 & (x-1)^2 \end{bmatrix},$$

which is a *canonical matrix polynomial*. Now the *elementary divisors* of $A(x)$ are $a_1(x) = 1$, $a_2(x) = x - 1$, and $a_3(x) = (x-1)^2 = x^2 - 2x + 1$, where $a_1(x) \mid a_2(x) \mid a_3(x)$. ◇

Definition 22. (<u>Rational Canonical Form of a Matrix</u>)

Definition 22(a). *The rational canonical form of a matrix $A \in M(n, F)$, is the matrix*

$$D = \begin{bmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_r \end{bmatrix},$$

where C_i, for $1 \le i \le r$, is the companion matrix of the elementary divisor $a_i(x)$ of the matrix polynomial $A(x)$. ◇

Definition 22(b). *Let $A \in M(n, F)$, where F is a field. Then A is similar to a unique matrix D, such that D is the direct sum of the companion matrices of a unique family of polynomials $q_1, q_2, q_3, \ldots, q_t \in F[x]$, such* *that $q_1 \,|\, q_2 \,|\, q_3 \,|\, \cdots \,|\, q_t$. The matrix D is said to be in rational canonical form, or is said to be the rational canonical form of the matrix A.* $\diamond$

Example 27. (Rational Canonical Form of a Matrix)

Using the matrix A of the previous example, Example 26, and Definition 22(a) of the rational canonical form of a matrix, we see that since the elementary divisors of the matrix polynomial $A(x)$ are $a_1(x) = 1$, $a_2 = x - 1$, and $a_3(x) = (x-1)^2 = x^2 - 2x + 1$, and since the companion matrices of these elementary divisors are

$$Com(a_1) \text{ does not exist }, \quad Com(a_2) = [\,1\,], \text{ and } Com(a_3) = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix},$$

it follows that the *rational canonical form* of the matrix A is the matrix

$$D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{bmatrix}. \quad \diamond$$

Definition 23. (Monomial or Weighted Permutation Matrix) *A monomial permutation matrix or a weighted permutation matrix is a matrix in which each row and each column contains exactly one non-zero entry.*

Example 28. (Monomial or Weighted Permutation Matrix)

The matrix $A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 2 & 0 & 0 \end{bmatrix} \in M(4, Z_{11})$ is a *monomial* or *weighted permutation matrix*. $\diamond$

Note 8.

If all the non-zero entries of a weighted permutation matrix are replaced with 1's, a permutation matrix is obtained, and all permutation matrices, weighted or not, correspond to permutations of indices.

For example, the permutation corresponding to the permutation matrix $B = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ maps the index k onto the index l if the non-zero entry of column k is in row l of the matrix B. So, in this case, the permutation $\tau = (1,3,4)(2)(5)$ corresponds to the permutation matrix B.

In the previous example, Example 28, the permutation $\sigma = (1,3,4,2)$ corresponds to the weighted permutation matrix A. $\diamond$

Note 9.

Every $n \times n$ matrix over a field is similar to its transpose.

For example consider the general 2×2 case of the matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(2, F)$.

If $b \neq 0$ then let $X = \begin{bmatrix} 1 & 0 \\ 0 & \frac{c}{b} \end{bmatrix} \in M(2, F)$. Since $\det(X) = \frac{c}{b}$ we need to consider two cases.

Case 1

If $c \neq 0$ then $\det(X) \neq 0$, so X is non- singular and X^{-1} exists, and so we have

$$AX = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{c}{b} \end{bmatrix} = \begin{bmatrix} a & c \\ c & \frac{dc}{b} \end{bmatrix}$$

and,

$$XA^T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{c}{b} \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a & c \\ c & \frac{dc}{b} \end{bmatrix}.$$

Therefore $AX = XA^T \Rightarrow X^{-1}AX = A^T$, and so A is similar to A^T.

Case 2

If $c \neq 0$ then $\det(X) = 0$ and so X is not invertible. However, there exists a matrix $Y = \begin{bmatrix} 0 & 1 \\ 1 & \frac{d-a}{b} \end{bmatrix} \in M(2, F)$ with $\det(Y) = -1 \neq 0$. Since Y is non-singular, Y^{-1} exists and we have

$$AY = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & \frac{d-a}{b} \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & \frac{d-a}{b} \end{bmatrix} = \begin{bmatrix} b & d \\ d & d(\frac{d-a}{b}) \end{bmatrix}$$

and,

$$YA^T = \begin{bmatrix} 0 & 1 \\ 1 & \frac{d-a}{b} \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & \frac{d-a}{b} \end{bmatrix} \begin{bmatrix} a & 0 \\ b & d \end{bmatrix} = \begin{bmatrix} b & d \\ d & d(\frac{d-a}{b}) \end{bmatrix}.$$

Therefore $AY = YA^T \Rightarrow Y^{-1}AY = A^T$, and so A is similar to A^T.

Now if $b = 0$ and $c = 0$ we have

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$$

and,

$$A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix},$$

so $A = A^T$ and A is similar to A^T.

If $b = 0$ and $c \neq 0$, then let $X = \begin{bmatrix} \frac{a-d}{c} & 1 \\ 1 & 0 \end{bmatrix} \in M(2, F)$. Since $\det(X) = -1 \neq 0$, then X is non-singular and X^{-1} exists, and so we have

$$AX = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \frac{a-d}{c} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} \frac{a-d}{c} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a(\frac{a-d}{c}) & a \\ a & c \end{bmatrix}$$

and,

$$XA^T = \begin{bmatrix} \frac{a-d}{c} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} \frac{a-d}{c} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} a(\frac{a-d}{c}) & a \\ a & c \end{bmatrix}.$$

So we have $AX = XA^T \Rightarrow X^{-1}AX = A^T$, and A is similar to A^T.

Therefore there exists a matrix $X \in GL(2, F)$ such that $X^{-1}AX = A^T$, and so it follows that any 2×2 matrix $A \in M(2, F)$ is similar to its transpose. ◇

The following definition will not be used until Section 7.

Definition 24. *(First Bass Stable Ring Condition) Let R be a ring. If for all $a, b \in R$, with $Ra + Rb = R$, there exists some $c \in R$ such that $R(a+cb) = R$, we say that R satisfies the first Bass stable range condition, or, equivalently, that R is a Bass ring.* $\diamond$

Note 10.

The following are some examples of rings that either satisfy or do not satisfy the first Bass stable range condition:

1. Any field or division ring satisfies the first Bass stable range condition.

2. If R is a Dedekind ring of arithmetic type, R may not satisfy the first Bass stable range condition.

3. Any Artinian ring is a Bass ring. $\diamond$

Section 3. Involutions in General

In the previous section, Section 2, an involution A was defined as a matrix in $GL(n, F)$, the general linear group of all invertible $n \times n$ matrices with entries over a field F, such that $A^2 = I_n$. In this section we will continue our examination of involutions by developing various general results regarding involutions and their products, and one very important result concerning matrices that are similar to involutions.

Proposition 1. *When studying involutions in $GL(n, F)$ only the elements of the group $\pm SL(n, F)$, the group of all invertible $n \times n$ matrices of determinant ± 1 over the field F, need to be considered.*

Proof (Proposition 1).

Let $A \in GL(n, F)$ be any arbitrary involution. Then

$$\det(A) \cdot \det(A) = \det(A^2) = \det(I) = 1,$$

and so it follows that $\det(A) = \pm 1$.

Hence if A is an involution in $GL(n, F)$ then $A \in \pm SL(n, F)$. $\diamond$

Proposition 2. *Any matrix that can be written as a product of two or more involutions has a determinant of ± 1.*

Proof (Proposition 2).

Let $B \in GL(n, F)$ be a matrix that can be written as a product of k involutions, say $A_1, A_2, A_3, \ldots, A_k$, where $A_i \in \pm SL(n, F)$ for each i.

So we have

$$B = A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_k \Rightarrow \det(B) = \det(A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_k) = \det(A_1) \cdot \det(A_2) \cdot \det(A_3) \cdot \ldots \cdot \det(A_k).$$

Now $\det(A_i) = \pm 1$ for each $i = 1, 2, 3, \ldots, k$, and so it follows that $\det(B) = \pm 1$.

Hence, if B can be written as a product of involutions then $B \in \pm SL(n, F)$ (This result also follows directly from the closure of the group $\pm SL(n, F)$ under multiplication). $\diamond$

By Proposition 1 and Proposition 2, it follows that when studying involutions and their products, we can narrow our discussion to matrices in $\pm SL(n, F)$, and so we don't need to consider all of $GL(n, F)$. We will make use of this fact later on, especially in Section 5.

Theorem 1. *Let $A \in \pm SL(n, F)$ be a matrix that can be written as a product of $k \geq 0$ involutions, and let $C \in \pm SL(n, F)$ be a matrix that is similar to A. Then C can also be written as a product of k involutions.*

Proof (Theorem 1).

Let $A \in \pm SL(n, F)$ be a matrix that can be written as a product of $k \geq 0$ involutions, and let $C \in \pm SL(n, F)$ be a matrix that is similar to A. Then there exists a matrix $B \in GL(n, F)$ such that $B^{-1}AB = C$.

Now if $k = 0$ then A isn't an involution. If we assume in this case that C is an involution then we have

$$B^{-1}AB = C \Rightarrow A = BCB^{-1} \Rightarrow A^2 = A \cdot A = (BCB^{-1})(BCB^{-1}) = BCCB^{-1} = BB^{-1} = I,$$

and so A must be an involution, which is a direct contradiction to our assumption. Hence C is also not an involution (i.e., C is the product of 0 involutions), and so the statement of the theorem holds for $k = 0$.

Now let $k = 1$. Then A is an involution and since $C = B^{-1}AB$, we have

$$C^2 = (B^{-1}AB)(B^{-1}AB) = B^{-1}AAB = B^{-1}B = I,$$

and so it follows that C is also an involution, (i.e., C is the product of 1 involution), and we have shown that the statement of the theorem holds for $k = 1$.

Assume now that the statement of the theorem holds for all $0 \leq k \leq p$, for some $p \in N, p \geq 1$. That is, if a matrix A can be written as the product of k involutions, where $0 \leq k \leq p$, then so can any matrix that is similar to A.

Let $k = p + 1$. Then A can be written as the product of $p + 1$ involutions, so $A = XY$, where X is the product of p involutions, and Y is itself an involution, and since C is similar to A we have

$$C = B^{-1}AB = B^{-1}(XY)B = (B^{-1}XB)(B^{-1}YB).$$

Now X is the product of p involutions and $B^{-1}XB$ is similar to X, and so by the induction hypothesis $B^{-1}XB$ can be written as the product of p involutions. Also, Y is an involution and $B^{-1}YB$ is similar to Y, so, again by the induction hypothesis, $B^{-1}YB$ is itself an involution. Therefore it follows that $C = (B^{-1}XB)(B^{-1}YB)$ can be written as the product of $p + 1$ involutions.

Hence if A can be written as the product of $p + 1$ involutions then so can any matrix similar to A, and so by induction the statement of the theorem holds for all $k \geq 0$. ◇

Section 4. Products of Two Involutions

In this section we will examine the special case of matrices that can be written as the product of exactly two involutions. To start our discussion let us consider the following example.

Example 30. *(A Product of Two Involutions)*

Let $A = \begin{bmatrix} 8 & 5 \\ 6 & 8 \end{bmatrix} \in \pm SL(2, Z_{11})$, and note that $B = \begin{bmatrix} 10 & 0 \\ 0 & 1 \end{bmatrix}$ and $C = \begin{bmatrix} 3 & 6 \\ 6 & 8 \end{bmatrix}$ are both involutions in $\pm SL(2, Z_{11})$, since

$$B^2 = \begin{bmatrix} 100 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } C^2 = \begin{bmatrix} 45 & 66 \\ 66 & 100 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Now since

$$BC = \begin{bmatrix} 10 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 3 & 6 \\ 6 & 8 \end{bmatrix} = \begin{bmatrix} 30 & 60 \\ 6 & 8 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ 6 & 8 \end{bmatrix} = A,$$

it follows that A can be written as the product of two involutions in $\pm SL(2, Z_{11})$, and so there exist matrices that can be written as the product of exactly two involutions. ◇

This example leads us to the first theorem of this section.

Theorem 2 (cf. [3]), [10]. *An $n \times n$ matrix over a field can be written as a product of two involutions if and only if it is non-singular and similar to its inverse.*

Proof (Theorem 2).

Let $A \in M(n, F)$, such that $A = BC$ where B and C are both involutions. Then since $\det(A) = \det(B)\det(C) \neq 0$, A is non-singular, and also $B = B^{-1}$, and $C = C^{-1}$, so we have

$$A^{-1} = (BC)^{-1} = C^{-1}B^{-1} = CB, \text{ and so}$$

$$B^{-1}AB = B^{-1}(BC)B = (B^{-1}B)(CB) = CB = A^{-1}.$$

Therefore, if $A \in M(n, F)$ can be written as the product of two involutions, then A is non-singular and similar to its inverse.

Now let $A \in GL(n, F)$ be a matrix that is similar to its inverse. So there exists some $B \in GL(n, F)$ such that $B^{-1}AB = A^{-1}$.

Also, we can write A in its rational canonical form D, where D is an $n \times n$ block diagonal matrix that is similar to A, say $D = diag(D_1, D_2, D_3, \ldots, D_m)$, where each block D_i, for $i = 1, 2, 3, \ldots, m$, is indecomposable, and D is unique up to the order in which the blocks D_1, D_2, D_3, $\ldots$, D_k occur. Note that since A is non-singular then by Note 1 in Section 2 so is D, and so D^{-1} does indeed exist.

Now since A is similar to D there exists some matrix $C \in GL(n, F)$ such that $C^{-1}AC = D \Rightarrow A = CDC^{-1}$.

So we have

$$A = CDC^{-1} \Rightarrow B^{-1}AB = B^{-1}CDC^{-1}B \Rightarrow A^{-1} = B^{-1}CDC^{-1}B \Rightarrow (CDC^{-1})^{-1} = B^{-1}CDC^{-1}B \Rightarrow$$

$$CD^{-1}C^{-1} = B^{-1}CDC^{-1}B \Rightarrow D^{-1} = (C^{-1}B^{-1}C)D(C^{-1}BC) \Rightarrow D^{-1} = (C^{-1}BC)^{-1}D(C^{-1}BC),$$

and we see that D is similar to its inverse.

Now by the transitivity of similarity, since A is similar to D, and D is similar to D^{-1}, it follows that A is similar to D^{-1}, and so if D^{-1} can be written as the product of two involutions, then, by Theorem 1 in Section 3, so can A.

Since, by Note 4 in Section 2, $D = diag(D_1, D_2, D_3, \ldots, D_m) \Rightarrow D^{-1} = diag(D_1^{-1}, D_2^{-1}, D_3^{-1}, \ldots, D_k^{-1})$, and D is similar to D^{-1}, where each block of D and D^{-1} is indecomposable, then, by Note 5, it follows that some of the D_i blocks are similar to their own inverses D_i^{-1}, while the rest come in pairs, where each member of the pair is similar to the inverse of the other.

For example if D_p is similar to D_q^{-1}, for some $p, q \in 1, 2, 3, \ldots, m$, then there exists some invertible matrix K of appropriate size such that

$$K^{-1}D_pK = D_q^{-1} \Rightarrow (K^{-1}D_pK)^{-1} = (D_q^{-1})^{-1} \Rightarrow K^{-1}D_p^{-1}K = D_q,$$

and so it follows that D_q must be similar to D_p^{-1}. So the block $diag(D_p^{-1}, D_q^{-1})$ in the $n \times n$ matrix D^{-1}, is similar to a block of the form $diag(D_q, D_q^{-1})$.

If we now assume that the first l blocks of D^{-1} are the blocks that are similar to their own inverses, then D_i^{-1} is similar to $(D_i^{-1})^{-1} = D_i$, for $1 \leq i \leq l$, and that the rest of the blocks of D^{-1} come in block pairs of the form $diag(D_p^{-1}, D_q^{-1})$, where D_p is similar to D_q^{-1} and D_q is similar to D_p^{-1}, then it follows that D^{-1} is similar to a block diagonal matrix M which is the direct sum of the first D_i blocks of D, with $1 \leq i \leq l$, and the blocks of the form $diag(D_q, D_q^{-1})$.

Now if we can show that each D_i, for $1 \leq i \leq l$, is the product of two involutions, and that each block of the form $diag(D_q, D_q^{-1})$ is the product of two involutions, then, by Note 6 in Section 2, M can be written as the product of two involutions, and so, by similarity and Theorem 1, so can D^{-1}.

Since $diag(D_q, D_q^{-1}) = \begin{bmatrix} D_q & 0 \\ 0 & D_q^{-1} \end{bmatrix} = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} 0 & D_q^{-1} \\ D_q & 0 \end{bmatrix}$, and

$$\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} \text{ and}$$

$$\begin{bmatrix} 0 & D_q^{-1} \\ D_q & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & D_q^{-1} \\ D_q & 0 \end{bmatrix} \begin{bmatrix} 0 & D_q^{-1} \\ D_q & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix},$$

it follows that $\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$, and $\begin{bmatrix} 0 & D_q^{-1} \\ D_q & 0 \end{bmatrix}$ are involutions, and so all the blocks of the form $diag(D_q, D_q^{-1})$ in M can be written as the product of two involutions.

Now let us consider the blocks of the form D_i, $1 \leq i \leq l$, where each D_i is similar to its own inverse. Each of these D_i blocks is also a block of D, the rational canonical form of A, and so each is the $k \times k$ companion matrix of some monic polynomial $f_i(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \in F[x]$, for suitable k. So

$$D_i = Com(f_i) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{bmatrix}, \text{ for } 1 \leq i \leq l.$$

Define $\overline{f_i}(x)$ by

$\overline{f_i}(x) = \frac{x^k}{a_0} f_i(\frac{1}{x}) = \frac{x^k}{a_0}(\frac{1}{x^k} + a_{k-1}\frac{1}{x^{k-1}} + a_{k-2}\frac{1}{x^{k-2}} + \cdots + a_1\frac{1}{x^1} + a_0) =$

$a_0^{-1}(1+a_{k-1}x+a_{k-2}x^2+\cdots+a_1x^{k-1}+a_0x^k) = a_0^{-1}+a_0^{-1}a_{k-1}x+a_0^{-1}a_{k-2}x^2+\cdots+a_0^{-1}a_1x^{k-1}+a_0^{-1}a_0x^k =$

$x^k + a_0^{-1}a_1x^{k-1} + a_0^{-1}a_2x^{k-2} + \cdots + a_0^{-1}a_{k-2}x^2 + a_0^{-1}a_{k-1}x + a_0^{-1}.$

Then the companion matrix of $\overline{f_i}$ is defined by the $k \times k$ matrix

$$Com(\overline{f_i}) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0^{-1} \\ 1 & 0 & \cdots & 0 & -a_0^{-1}a_{k-1} \\ 0 & 1 & \cdots & 0 & -a_0^{-1}a_{k-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_0^{-1}a_1 \end{bmatrix}, \text{ for } 1 \le i \le l.$$

Now we can note that

$$D_i^{-1} = [Com(f_i)]^{-1} = \begin{bmatrix} -a_0^{-1}a_1 & 1 & 0 & \cdots & 0 & 0 \\ -a_0^{-1}a_2 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -a_0^{-1}a_{k-2} & 0 & 0 & \cdots & 1 & 0 \\ -a_0^{-1}a_{k-1} & 0 & 0 & \cdots & 0 & 1 \\ -a_0^{-1} & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}, \text{ for } 1 \le i \le l,$$

and so if we let J_k be the invertible $k \times k$ permutation matrix defined by

$$J_k = J_k^{-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix},$$

then since $J_k^{-1}D_i^{-1}J_k = J_k^{-1}[Com(f_i)]^{-1}J_k = Com(\overline{f_i})$, it follows that $D_i^{-1} = [Com(f_i)]^{-1}$ is similar to $Com(\overline{f_i})$, for $1 \le i \le l$.

But now since we assumed that $D_i = Com(f_i)$ is similar to its inverse $D_i^{-1} = [Com(f_i)]^{-1}$, and we showed that $D_i^{-1} = [Com(f_i)]^{-1}$ is similar to $Com(\overline{f_i})$, then by the transitivity of similarity it follows that $D_i = Com(f_i)$ is similar to $Com(\overline{f_i})$, for $1 \le i \le l$.

So the $n \times n$ matrix M is now similar to an $n \times n$ matrix L which is the direct sum of the first l blocks of the form $Com(\overline{f_i})$, for $1 \le i \le l$, and the blocks of the form $diag(D_q, D_q^{-1})$. But this means that D^{-1} is similar to L, and so D must also be similar to L, and since D is similar to A, then A must also be similar to the block matrix L.

So the matrix L, since it is a block matrix similar to A where each block is the companion matrix of a monic polynomial $\overline{f_i}(x)$ over F, is also a rational canonical form of A, and by the uniqueness of the rational canonical form of a matrix, we have

$$D = L \Rightarrow$$

$$diag[D_1, D_2, \ldots, D_l, diag(D_p, D_p^{-1}), \ldots, diag(D_q, D_q^{-1})] =$$

$$diag[Com(\overline{f_1}), Com(\overline{f_2}), \ldots, Com(\overline{f_l}), diag(D_p, D_p^{-1}), \ldots, diag(D_q, D_q^{-1})],$$

and so it must be the case that

$$D_i = Com(\overline{f_i}) \Rightarrow Com(f_i) = Com(\overline{f_i}) \Rightarrow \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0^{-1} \\ 1 & 0 & \cdots & 0 & -a_0^{-1}a_{k-1} \\ 0 & 1 & \cdots & 0 & -a_0^{-1}a_{k-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_0^{-1}a_1 \end{bmatrix}, \text{ for } 1 \leq i \leq l.$$

Therefore it follows that $a_0 = a_0^{-1}$, $a_1 = a_0^{-1}a_{k-1}$, $\ldots$, $a_{k-2} = a_0^{-1}a_2$, $a_{k-1} = a_0^{-1}a_1$, and, in general,

$$a_0 = a_0^{-1} \Rightarrow a_0^2 = 1, \text{ and}$$

$$a_{k-j} = a_0^{-1}a_j \Rightarrow a_{k-j} = a_0 a_j \Rightarrow a_0 a_j - a_{k-j} = 0, \text{ for } 1 \leq j \leq k-1.$$

Consider now the $k \times k$ permutation matrix J_k defined earlier by

$$P_k = P_k^{-1} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Clearly J_k is an involution and so $J_k^2 = I_k$, and also for suitable k we have

$$D_iJ_k = Com(f_i)J_k = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{k-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{k-1} \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} -a_0 & 0 & 0 & \cdots & 0 & 0 \\ -a_1 & 0 & 0 & \cdots & 0 & 1 \\ -a_2 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \vdots & \vdots \\ -a_{k-2} & 0 & 1 & \cdots & 0 & 0 \\ -a_{k-1} & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}, \text{ for } 1 \leq i \leq l.$$

Now

$$(D_iJ_k)^2 = \begin{bmatrix} -a_0 & 0 & 0 & \cdots & 0 & 0 \\ -a_1 & 0 & 0 & \cdots & 0 & 1 \\ -a_2 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \vdots & \vdots \\ -a_{k-2} & 0 & 1 & \cdots & 0 & 0 \\ -a_{k-1} & 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} -a_0 & 0 & 0 & \cdots & 0 & 0 \\ -a_1 & 0 & 0 & \cdots & 0 & 1 \\ -a_2 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdot^{\cdot^{\cdot}} & \vdots & \vdots \\ -a_{k-2} & 0 & 1 & \cdots & 0 & 0 \\ -a_{k-1} & 1 & 0 & \cdots & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} a_0^2 & 0 & 0 & \cdots & 0 & 0 \\ a_0a_1 - a_{k-1} & 1 & 0 & \cdots & 0 & 0 \\ a_0a_2 - a_{k-2} & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_0a_{k-2} - a_2 & 0 & 0 & \cdots & 1 & 0 \\ a_0a_{k-1} - a_1 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} = I_k, \text{ for } 1 \leq i \leq l,$$

and so D_iJ_k, for $1 \leq i \leq l$, is an involution.

But then

$$(D_iJ_k)J_k = D_i(J_k)^2 = D_i, \text{ for } 1 \leq i \leq l,$$

is a product of two involutions.

So we have shown that each of the blocks of the form D_i, $1 \leq i \leq l$, in M that are similar to their own inverses can be written as the product of two involutions, and earlier we showed that the blocks of the form $diag(D_q, D_q^{-1})$ in M can be written as a product of two involutions. Since all of the blocks of the block diagonal matrix M can be written as a product of two involutory matrices then, by Note 6 in Section 2, it follows that M itself can be written as the product of two involutions. Now, since D^{-1} is similar to M, then by Theorem 1 in Section 3, D^{-1} can be written as the product of two involutions, and since A is similar to D^{-1} then, again by Theorem 1, A can also be written as the product of two involutions.

Hence if $A \in GL(n, F)$ is a matrix that is similar to its inverse then A can be written as the product of two involutions.

So we have shown that an $n \times n$ matrix over a field can be written as the product of two involutions if and only if it is non-singular and similar to its inverse. ◇

Example 31. *(A Product of Two Involutions)*

Consider the matrix $A = \begin{bmatrix} 8 & 5 \\ 6 & 8 \end{bmatrix} \in \pm SL(2, Z_{11})$. In Example 29 we showed that A could be written as the product of two involutions. Now $A^{-1} = \begin{bmatrix} 8 & 6 \\ 5 & 8 \end{bmatrix}$, and

$$B^{-1}A^{-1}B = BA^{-1}B = B\begin{bmatrix} 8 & 6 \\ 5 & 8 \end{bmatrix}\begin{bmatrix} 10 & 0 \\ 0 & 1 \end{bmatrix} = B\begin{bmatrix} 80 & 6 \\ 50 & 8 \end{bmatrix} = B\begin{bmatrix} 3 & 6 \\ 6 & 8 \end{bmatrix} = BC = A,$$

and so it follows that A is similar to its inverse. ◇

The next theorem is very similar to Theorem 2, and, as will be shown later in Proposition 3, its conditions are actually equivalent to those of Theorem 2.

Theorem 3 (cf. [2]). *An $n \times n$ matrix over a field can be written as a product of two involutions if and only if it is non-singular and involutorily similar to its inverse.*

Proof (Theorem 3).

Let $A \in M(n, F)$ be the product of two involutions, B and C, both in $GL(n, F)$. Then $A = BC$, where $B^2 = I_n$ and $C^2 = I_n$.

Since $\det(A) = \det(B)\det(C) \neq 0$, then A is non-singular, and so $A \in GL(n, F)$.

Also we have

$$A = BC = (CC)BC = C(CB)C = C(B^{-1}C^{-1})^{-1}C = C(BC)^{-1}C = CA^{-1}C = C^{-1}A^{-1}C,$$

and so if $A \in M(n, F)$ can be written as the product of two involutions then A is non-singular and involutorily similar to its inverse.

Now let $A \in GL(n, F)$ be a matrix that is involutorily similar to its inverse. So there exists some involution $X \in GL(n, F)$ such that $A = X^{-1}A^{-1}X \Rightarrow A = XA^{-1}X$.

Since $A = XA^{-1}X$ then we have

$$A = XA^{-1}X \Rightarrow XA = A^{-1}X \Rightarrow XA = (X^{-1}A)^{-1} \Rightarrow XA = (XA)^{-1},$$

and so we have shown that XA is also an involution.

But now we see that

$$X(XA) = (XX)A = A,$$

and so it follows that if A is involutorily similar to its inverse then A can be written as the product of two involutions. ◇

Example 29 is an example of Theorem 3, since the matrix A that is used is not only similar to its inverse, but it is also involutorily similar to its inverse. This observation leads us to the following proposition.

Proposition 3 (cf. [2]). *Let $A \in GL(n, F)$. Then A is similar to its inverse if and only if A is involutorily similar to its inverse, and so the conditions of Theorem 2 and Theorem 3 are equivalent.*

Proof (Proposition 3).

Let $A \in GL(n, F)$, such that A is similar to its inverse. Then, by Theorem 1, A can be written as the product of two involutions in $GL(n, F)$, and so, by Theorem 2, it follows that A must be involutorily similar to its inverse.

On the other hand, let $A \in GL(n, F)$, such that A is involutorily similar to its inverse. Then A is also similar to its inverse.

Thus for any matrix $A \in GL(n, F)$, A is similar to its inverse if and only if A is involutorily similar to its inverse, and so the conditions of Theorems 2 and 3 are equivalent. ◇

The next example shows that in many cases not only can a matrix be factored into two involutions, but it can be factored into two unitary involutions.

Example 32. *(A Unitary Matrix that is the Product of Two Unitary Involutions)*

Let $X = \begin{bmatrix} 0 & -1 & -3 \\ -3 & 1 & 0 \\ -1 & -1 & -2 \end{bmatrix} \in M(3, Z_7)$.

Then

$$X^* = adj(X) = \begin{bmatrix} \begin{vmatrix} 1 & 0 \\ -1 & -1 \end{vmatrix} & -\begin{vmatrix} -3 & 0 \\ -1 & -2 \end{vmatrix} & \begin{vmatrix} -3 & 1 \\ -1 & -1 \end{vmatrix} \\ -\begin{vmatrix} -1 & -3 \\ -1 & -2 \end{vmatrix} & \begin{vmatrix} 0 & -3 \\ -1 & -2 \end{vmatrix} & -\begin{vmatrix} 0 & -1 \\ -1 & -1 \end{vmatrix} \\ \begin{vmatrix} -1 & -3 \\ 1 & 0 \end{vmatrix} & \begin{vmatrix} 0 & -3 \\ -3 & 0 \end{vmatrix} & \begin{vmatrix} 0 & -1 \\ -3 & 1 \end{vmatrix} \end{bmatrix}^T = \begin{bmatrix} -2 & -6 & 4 \\ 1 & -3 & 1 \\ 3 & 9 & -3 \end{bmatrix}^T =$$

$$\begin{bmatrix} -2 & 1 & 3 \\ -6 & -3 & 9 \\ 4 & 1 & -3 \end{bmatrix} = \begin{bmatrix} -2 & 1 & 3 \\ 1 & -3 & 2 \\ -3 & 1 & -3 \end{bmatrix} \in M(3, Z_7).$$

Now

$$X^*X = \begin{bmatrix} -2 & 1 & 3 \\ 1 & -3 & 2 \\ -3 & 1 & -3 \end{bmatrix} \begin{bmatrix} 0 & -1 & -3 \\ -3 & 1 & 0 \\ -1 & -1 & -2 \end{bmatrix} = \begin{bmatrix} -3-3 & 2+1-3 & 6-6 \\ 9-2 & -1-3-2 & -3-4 \\ -3+3 & 3+1+3 & 9+6 \end{bmatrix} =$$

$$\begin{bmatrix} -6 & 0 & 0 \\ 7 & -6 & -7 \\ 0 & 7 & 15 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so X is a unitary matrix.

From Example 10 in Section 2 we know that

$$A = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} \in M(3, Z_7)$$

is a unitary involution, and if we let

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 3 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} \in M(3, Z_7),$$

then we have

$$B^2 = \begin{bmatrix} 1 & 0 & 0 \\ 3 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 3 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 3-3 & 1 & 0 \\ 2-2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so it follows that B is an involution.

Also,

$$B^* = adj(B) = \begin{bmatrix} \begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix} & -\begin{vmatrix} 3 & 0 \\ 2 & -1 \end{vmatrix} & \begin{vmatrix} 3 & -1 \\ 2 & 0 \end{vmatrix} \\ -\begin{vmatrix} 0 & 0 \\ 0 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 2 & -1 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 2 & 0 \end{vmatrix} \\ \begin{vmatrix} 0 & 0 \\ -1 & 0 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 3 & 0 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 3 & -1 \end{vmatrix} \end{bmatrix}^T = \begin{bmatrix} 1 & 3 & 2 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}^T =$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 3 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} = B,$$

and so $B^*B = BB = I_3$, which means that B is also a unitary matrix. Hence, $B \in M(3, Z_7)$ is a unitary involution.

Now we have

$$AB = \begin{bmatrix} -2 & 1 & 3 \\ 0 & -1 & 0 \\ -1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 3 & -1 & 0 \\ 2 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -2+3+6 & -1 & -3 \\ -3 & 1 & 0 \\ -1+3+4 & -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & -1 & -3 \\ -3 & 1 & 0 \\ -1 & -1 & -2 \end{bmatrix} = X,$$

and so $X \in M(3, Z_7)$ is a unitary matrix that can be written as the product of two unitary involutions. $\diamond$

Note 11.

Consider the matrix $X = \begin{bmatrix} 0 & -1 & -3 \\ -3 & 1 & 0 \\ -1 & -1 & -2 \end{bmatrix} \in M(3, Z_7)$.

In the previous example we showed that X is a unitary matrix that can be written as the product of two unitary involutions, and we calculated $X^* = \begin{bmatrix} -2 & 1 & 3 \\ 1 & -3 & 2 \\ -3 & 1 & -3 \end{bmatrix}$, the adjoint of X.

Now we can observe that there exists a matrix $Y = \begin{bmatrix} -2 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & -3 \end{bmatrix} \in GL(3, Z_7)$, with $Y^{-1} = \begin{bmatrix} 3 & 0 & 0 \\ 3 & -3 & -1 \\ 1 & 0 & 2 \end{bmatrix}$, such that

$$Y^{-1}XY = \begin{bmatrix} 3 & 0 & 0 \\ 3 & -3 & -1 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & -1 & -3 \\ -3 & 1 & 0 \\ -1 & -1 & -2 \end{bmatrix} Y = \begin{bmatrix} 0 & -3 & -2 \\ 3 & 2 & 0 \\ -2 & -3 & 0 \end{bmatrix} \begin{bmatrix} -2 & 0 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & -3 \end{bmatrix} =$$
$$\begin{bmatrix} -2 & -6 & -6+6 \\ -6 & 4 & 2 \\ 4 & -6 & -3 \end{bmatrix} = \begin{bmatrix} -2 & 1 & 3 \\ 1 & -3 & 2 \\ -3 & 1 & -3 \end{bmatrix} = X^*,$$

and so the matrix X is also similar to its adjoint. $\diamond$

The previous example considered together with Note 11, provides an illustration of the following theorem, Theorem 4.

Theorem 4. *If A is an $n \times n$ unitary matrix over a field F that is the product of two involutions then A is similar to its adjoint A^*.*

Proof (Theorem 4).

Let $A \in M(n, F)$ be a unitary matrix such that A is the product of two involutions. Then, by Theorem 2, we know that A is non-singular, so A^{-1} exists, and we also know that A is similar to A^{-1}.

Now since A is unitary, $A^*A = I$, and so A^* is a left inverse of A. But A is square, so any left inverse of A is also a right inverse, and by the uniqueness of matrix inverses it follows that $A^* = A^{-1}$ ($A^*A = I \Rightarrow A^*(AA^{-1}) = A^{-1} \Rightarrow A^* = A^{-1}$).

Now since A is similar to its inverse, and $A^* = A^{-1}$, it follows that A is also similar to its adjoint.

Hence if $A \in M(n, F)$ is a unitary matrix that can be written as the product of two involutions then A is similar to its adjoint, A^*. $\diamond$

The following proposition, Proposition 4, gives more examples of matrices that can be written as the product of exactly two involutions.

Proposition 4 (cf. [3]). *Every 2×2 matrix A over a field F with $\det(A) = 1$ that is not an involution is the product of two involutory matrices over F.*

Proof (Proposition 4).

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M(2, F)$ be a matrix with $\det(A) = 1$, such that A itself is not an involution. So $A \in \pm SL(2, F)$, and $A^{-1} \neq A$.

Since $\det(A) = 1$ then $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, and there exists a matrix $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in GL(2, F)$, with $B^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ such that

$$B^{-1}A^TB = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} B = \begin{bmatrix} b & d \\ -a & -c \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = A^{-1},$$

and so it follows that A^T is similar to A^{-1}.

Now in Section 2, Note 9, we showed that every 2×2 matrix over a field is similar to its transpose, so A is similar to A^T. But A^T is also similar to A^{-1}, and so by the transitivity of similarity it follows that A is similar to A^{-1}. Hence, by Theorem 2, A can be written as the product of exactly two involutions over the field F.

Thus if A is a 2×2 matrix over a field F with $\det(A) = 1$, such that A itself is not an involution, then A can be written as the product of exactly two involutory matrices over F. ◇

So far in this section we have concerned ourselves with special matrices that can be written as the product of exactly two involutory matrices. In the next example we will show that two involutions do not always suffice, and that sometimes a matrix cannot be written as the product of two involutions but can be written as the product of three or more involutions.

Example 33. *(A Product of not Fewer than Three Involutions)*

Consider the cyclic matrix $A = \begin{bmatrix} -2 & 0 & -3 \\ 0 & 2 & -2 \\ -2 & -1 & 0 \end{bmatrix} \in M(3, Z_7)$ of Example 14 in Section 2. Then, as was shown in that example, A is similar to the companion matrix $Com(f) = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix}$ of the irreducible polynomial $f(x) = x^3 + 2x + 1 \in Z_7[x]$. Now since A is similar to $Com(f)$, then, by Theorem 1 in Section 2, it follows that if $Com(f)$ can be written as the product of k involutions then so can A.

Since

$$[Com(f)]^2 = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & -2 & -1 \\ 1 & 0 & -2 \end{bmatrix} \neq I_3,$$

then it follows that $Com(f)$ is not itself an involution, and so neither is A.

Also, since $Com(f)$ is non-singular, $[Com(f)]^{-1} = \begin{bmatrix} -2 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix}$ exists, and, by Theorem 2, $Com(f)$ can be written as the product of two involutions over Z_7 if and only if it is similar to its inverse $[Com(f)]^{-1}$.

Let us assume that $Com(f)$ can be written as the product of two involutions, so $Com(f)$ is similar to $[Com(f)]^{-1}$. Then there exists some non-singular matrix $D = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in GL(3, Z_7)$, such that

$$D^{-1}[Com(f)]D = [Com(f)]^{-1} \Rightarrow [Com(f)]D = D[Com(f)]^{-1} \Rightarrow$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} -2 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} -g & -h & -i \\ a-2g & b-2h & c-2i \\ d & e & f \end{bmatrix} = \begin{bmatrix} -2a-c & a & b \\ -2d-f & d & e \\ -2g-i & g & h \end{bmatrix}$$

Since the above matrices are equivalent only when $e = g = d = h = f = -a = -c = -i = b = 0 \Rightarrow a = b = c = d = e = f = g = h = i = 0$, then it follows that

$$D = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

But then $\det(D) = 0$, so D is singular, which means that D^{-1} doesn't exist and so there exists no invertible matrix $D \in GL(3, Z_7)$ such that $D^{-1}[Com(f)]D = [Com(f)]^{-1}$, and so $Com(f)$ cannot be similar to $[Com(f)]^{-1}$. Therefore our assumption that $Com(f)$ can be written as the product of exactly two involutions is incorrect, and so it follows that A also cannot be written as the product of two involutions.

Now let the matrix $B \in M(3, Z_7)$ be defined by $B = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, and let the matrix $C \in M(3, Z_7)$ be defined by $C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

Then $B^2 = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3$, and so B is an involution.

Now $C^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \neq I_3$, and so C is not an involution.

Since $\det(C) = 1$, then C is non-singular and so C^{-1} exists and is defined by $C^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$. Also, there exists a matrix $X = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} \in GL(3, Z_7)$, with $X^{-1} = \begin{bmatrix} -2 & -1 & -2 \\ -1 & -2 & -2 \\ -2 & -2 & -1 \end{bmatrix}$ such that

$$X^{-1}CX = \begin{bmatrix} -2 & -1 & -2 \\ -1 & -2 & -2 \\ -2 & -2 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} X = \begin{bmatrix} -1 & -2 & -2 \\ -2 & -2 & -1 \\ -2 & -1 & -2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = C^{-1}.$$

Now since $X^{-1}CX = C^{-1}$, then C is similar to its inverse, and by Theorem 2 it follows that C can be written as the product of two involutions in $GL(3, Z_7)$. Say $C = YZ$, where Y and Z are both involutions in $\pm SL(3, Z_7)$.

So we have

$$BYZ = BC = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} = Com(f),$$

and thus we have shown that $Com(f)$ can be written as the product of exactly three involutions in $\overset{+}{-} SL(3, Z_7)$, and so, by similarity and Theorem 1 of Section 3, so can the matrix A. Therefore the matrix $A \in GL(3, Z_7)$ is an example of a matrix that cannot be written as a product of fewer than three involutions. ◇

The previous example shows that not all matrices that can be written as the product of involutions can be written as the product of exactly two involutions; for some matrices more than two involutions are needed. This observation leads us to the main question of this paper as was posed in the introduction. That is, *does there exist some smallest positive integer k, such that any matrix in $\overset{+}{-} SL(n, F)$ which is the product of involutions, can be written as the product of at most k involutions, and if such an integer does in fact exist, what is it?* This question and its answer compose the main topic of the next section, Section 5.

Section 5. Products of Four Involutions

In this section we will state and prove the *Four Involutions Theorem* which is the main theorem of this paper, and which also answers the question posed in the introduction as to what is the smallest number of involutory factors required in the factorization of an arbitrary matrix over a field with determinant ± 1 into a product of involutions. However, before we state and prove this theorem, let us consider a matrix that can be written as the product of not fewer than four involutions, and thus show that number of involutions needed in any factorization into a product of involutory matrices is at least four.

Example 34. *(A Product of not Fewer than Four Involutions)*

Consider the matrix $A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \in M(3, Z_7)$. Then $\det(A) = 2^3 = 8 = 1$, and so A can be written as the product of some number of involutions over Z_7.

Since

$$A^2 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} -3 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -3 \end{bmatrix} \neq I_3,$$

then A is not an involution.

Now A is non-singular so $A^{-1} = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix}$ exists, and, by Theorem 2 of Section 4, A can be written as the product of exactly two involutions over Z_7 if and only if it is similar to A^{-1}. However, if A is similar to A^{-1} then there exists some invertible matrix $X = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in GL(3, Z_7)$, such that $X^{-1}AX = A^{-1}$.

So we have

$$X^{-1}AX = A^{-1} \Rightarrow AX = XA^{-1} \Rightarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{bmatrix} \Rightarrow$$

$$\begin{bmatrix} 2a & 2b & 2c \\ 2d & 2e & 2f \\ 2g & 2h & 2i \end{bmatrix} = \begin{bmatrix} 4a & 4b & 4c \\ 4d & 4e & 4f \\ 4g & 4h & 4i \end{bmatrix},$$

which is only true when $a = b = c = d = e = f = g = h = i = 0$. But this means that $X = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, and so $\det(X) = 0$, and X^{-1} does not exist, therefore our assumption that A is similar to A^{-1} is incorrect. Since A is not similar to its inverse then it follows, by Theorem 2, that A cannot be written as the product of exactly two involutions.

Let us suppose now that A can be written as the product of exactly three involutions. Say $A = BCD$, where B, C and D are all involutions in $\pm\, SL(3, Z_7)$.

Then we have

$$A = BCD \Rightarrow \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = BCD \Rightarrow 2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = BCD \Rightarrow 2I_3 = BCD \Rightarrow$$

$$2I_3D^{-1} = BCDD^{-1} \Rightarrow 2I_3D = BC \Rightarrow 2D = BC,$$

and so $2D \in M(3, Z_7)$ can be written as the product of two involutions which means that, by Theorem 2, $2D$ is similar to its inverse $(2D)^{-1} = 2^{-1}D^{-1} = 2^{-1}D$. So there exists some invertible matrix $K \in GL(3, Z_7)$ such that

$$K^{-1}(2D)K = 2^{-1}D \Rightarrow 2K^{-1}(2D)K = 22^{-1}D \Rightarrow K^{-1}(22D)K = D \Rightarrow K^{-1}(4D)K = D,$$

and so it follows that $4D$ is similar to D.

Now D is an involution so $\det(D) = \underline{+}1$ which means that D must be similar (up to the permutation of columns) to one of the following matrices in $M(3, Z_7)$:

(a) $\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = -I_3 = I_0 \oplus -I_3 = I_0 \oplus -I_{3-0}$, or

(b) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = I_1 \oplus -I_2 = I_1 \oplus -I_{3-1}$, or

(c) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = I_2 \oplus -I_1 = I_2 \oplus -I_{3-2}$, or

(d) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3 = I_3 \oplus -I_0 = I_3 \oplus -I_{3-3}$,

so D is similar to some matrix of the form $I_k \oplus -I_{3-k}$ for some $k = 0, 1, 2, 3$. But then $4D$ must be similar to $4(I_k \oplus -I_{3-k}) = 4I_k \oplus -4I_{3-k}$ for some $k = 0, 1, 2, 3$, and so by the transitivity of similarity, since D is also similar to $4D$, it follows that $I_k \oplus -I_{3-k}$ is similar to $4I_k \oplus -4I_{3-k}$ for some $k = 0, 1, 2, 3$. Also, $I_k, -I_{3-k}, 4I_k, -4I_{3-k}$ for $k = 0, 1, 2, 3$, are all *Jordan canonical matrices* and so they are block indecomposable. Now by Note 5 in Section 2 we know that if two block diagonal matrices are similar and their blocks are block indecomposable, then their blocks are similar in pairs, and so it follows that the blocks of $I_k \oplus -I_{3-k}$ and $4I_k \oplus -4I_{3-k}$ must be similar in pairs for some $k = 0, 1, 2, 3$.

Now, for $k = 0$, $I_0 \oplus -I_3$ is similar to $4I_0 \oplus -4I_3$, and since I_0 is clearly similar to itself, it follows that $-I_3$ must be similar to $-4I_3$. So there exists some invertible matrix $M = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in GL(3, Z_7)$, such that $M^{-1}(-I_3)M = -4I_3$.

So we have

$$M^{-1}(-I_3)M = -4I_3 \Rightarrow -I_3M = M(-4I_3) \Rightarrow \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} =$$

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} -4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{bmatrix} \Rightarrow \begin{bmatrix} -a & -b & -c \\ -d & -e & -f \\ -g & -h & -i \end{bmatrix} = \begin{bmatrix} -4a & -4b & -4c \\ -4d & -4e & -4f \\ -4g & -4h & -4i \end{bmatrix},$$

which is only true when $a = b = c = d = e = f = g = h = i = 0$. But this means that $M = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, so M is not invertible, and thus $-I_3$ cannot possibly be similar to $-4I_3$. Hence for $k = 0$ it follows that $I_k \oplus -I_{3-k}$ is not similar to $4I_k \oplus -4I_{3-k}$.

For $k = 1$, since $I_1 \oplus -I_2$ is similar to $4I_1 \oplus -4I_2$ then, by matching the dimensions of the corresponding blocks, it follows that I_1 must be similar to $4I_1$ and that $-I_2$ must be similar to $-4I_2$. Since $I_1 = [1]$ is similar to $4I_1 = [4]$, then there exists some matrix $M = [a] \in GL(1, Z_7)$, such that $M^{-1}[1]M = [4]$.

So we have

$$M^{-1}[1]M = [4] \Rightarrow [1]M = M[4] \Rightarrow [1][a] = [a][4] \Rightarrow [a] = [4a]$$

$$\Rightarrow a = 4a \Rightarrow -3a = 0 \Rightarrow 4a = 0 \Rightarrow a = 0 \text{ (since we are in the field } F).$$

But then $M = [0]$, which is not invertible, and so I_1 cannot possibly be similar to $4I_1$. Hence for $k = 1$ it follows that $I_k \oplus -I_{3-k}$ is not similar to $4I_k \oplus -4I_{3-k}$.

For $k = 2$, since $I_2 \oplus -I_1$ is similar to $4I_2 \oplus -4I_1$, by matching the dimensions of the corresponding blocks, it follows that I_2 must be similar to $4I_2$ and that $-I_1$ must be similar to $-4I_1$. Since $-I_1 = [-1]$ is similar to $-4I_1 = [-4]$, then there must exist some matrix $M = [a] \in GL(1, Z_7)$, such that $M^{-1}[-1]M = [-4] \Rightarrow -M^{-1}[1]M = -[4] \Rightarrow M^{-1}[1]M = [4]$, but, just as in the case when $k = 1$, this is impossible, and so $I_2 \oplus -I_1$ cannot possibly be similar to $4I_2 \oplus -4I_1$. Hence for $k = 2$ it follows that $I_k \oplus -I_{3-k}$ is not similar to $4I_k \oplus -4I_{3-k}$.

Finally, for $k = 3$, $I_3 \oplus -I_0$ is similar to $4I_3 \oplus -4I_0$, and since $-I_0$ is clearly similar to itself, it follows that I_3 must be similar to $4I_3$. So there exists some invertible matrix $M = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in GL(3, Z_7)$, such that $M^{-1}(I_3)M = 4I_3 \Rightarrow -M^{-1}I_3M = -4I_3 \Rightarrow M^{-1}(-I_3)M = -4I_3$, but, just as in the case when $k = 0$, this is impossible, and so I_3 cannot possibly be similar to $4I_3$. Hence for $k = 3$ it follows that $I_k \oplus -I_{3-k}$ is not similar to $4I_k \oplus -4I_{3-k}$.

Since we have shown that for all $k = 0, 1, 2, 3$, $I_k \oplus -I_{3-k}$ is not similar to $4I_k \oplus -4I_{3-k}$, then we have a contradiction, and so our assumption that A can be written as the product of exactly three involutions in $\pm SL(n, F)$ is incorrect.

So far, we have shown that A cannot be written as the product of one, two, or three involutions, and so all that remains to be shown is that A can be written as the product of exactly four involutions.

Let $W = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \in M(3, Z_7)$. Then

$$W^2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so W is an involution.

Let $X = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in M(3, Z_7)$. Then

$$X^2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so X is an involution.

Let $Y = \begin{bmatrix} 0 & 0 & -3 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{bmatrix} \in M(3, Z_7)$. Then

$$Y^2 = \begin{bmatrix} 0 & 0 & -3 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -3 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -6 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so Y is an involution.

Finally let $Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -3 & 0 \end{bmatrix} \in M(3, Z_7)$. Then

$$Z^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -3 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -3 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & -6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3,$$

and so Z is an involution.

Now

$$WXYZ = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} YZ = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & -3 \\ 0 & 1 & 0 \\ 2 & 0 & 0 \end{bmatrix} Z =$$

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -3 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & -3 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = A,$$

and so $A \in M(3, Z_7)$ is an example of a matrix that can be written as the product of exactly four involutions, and cannot be written as the product of one, two, or three involutions. ◇

In the above example we showed that there do exist matrices that cannot be written as the product of two or three involutions, and that sometimes four, or possibly more, involutions are needed in the factorization of a matrix. As we will see in the following theorem, the *Four Involutions Theorem*, it turns out that any matrix in $^{+}_{-}SL(n, F)$, where F is a field, can be factored as the product of not more than four involutions, and so four involutions suffice in each and every case.

Theorem 5 (The Four Involutions Theorem) (cf. [9], [10], [3]). Let A be any $n \times n$ matrix in $^{+}_{-}\, SL(n, F)$, where F is a field. *Then A can be written as the product of it at most four involutory matrices over F.*

Proof (Theorem 5).

Let $A \in {}^{+}_{-}SL(n, F)$. From the theory of rational canonical forms (see Definition 22 in Section 2), we know that A is similar to a block diagonal matrix of the form $A' = diag(D_1, D_2, D_3, \ldots, D_k)$, where $n_1 + n_2 + n_3 + \ldots + n_k = n$, and each D_i block, for $i = 1, 2, 3, \ldots k$, is the companion matrix of an irreducible polynomial over F. From Theorem 1 in Section 3, we know that if we can show that A' can be written as the product of at most four involutions over F, then, by similarity, so can A.

Since $A' = diag(D_1, D_2, D_3, \ldots, D_k)$, where each D_i block is the companion matrix of an irreducible polynomial over the field F, it follows that some of these D_i blocks, say the first l of them, are square matrices of order at least 2, of the form

$$D_i = \begin{bmatrix} 0 & 0 & \cdots & 0 & d_i \\ 1 & 0 & \cdots & 0 & * \\ 0 & 1 & \cdots & 0 & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \end{bmatrix} = \begin{bmatrix} 0 & d_i \\ I & B_i \end{bmatrix}, \text{ for } i = 1, 2, 3, \ldots, l,$$

where 0 and I are the appropriate zero and identity matrices, respectively, and B is a column matrix of suitable dimension, while the remaining $k - l$ D_i blocks in A' are 1×1 matrices of the form

$$D_i = [d_i], \text{ for } i = l+1, l+2, \ldots, k.$$

If we let L denote the direct sum of all these 1×1 blocks of A', then L is a block diagonal matrix of the form

$$L = D_{l+1} \oplus D_{l+2} \oplus D_{l+2} \oplus \ldots \oplus D_k = \begin{bmatrix} d_{l+1} & 0 & 0 & \cdots & 0 \\ 0 & d_{l+2} & 0 & \cdots & 0 \\ 0 & 0 & d_{l+3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_k \end{bmatrix},$$

and so A' becomes

$$A' = diag(D_1, D_2, \ldots, D_l, D_{l+1}, \ldots, D_k) = D_1 \oplus D_2 \oplus \ldots \oplus D_l \oplus D_{l+1} \oplus \ldots \oplus D_k = D_1 \oplus D_2 \oplus \ldots \oplus D_l \oplus L =$$

$$\begin{bmatrix} 0 & d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ I & B_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & d_2 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & B_2 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & d_l & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & I & B_l & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{l+1} & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{l+2} & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_{l+3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & \cdots & d_k \end{bmatrix},$$

where the 0's and I's denote the zero and identity matrices, respectively, and are all of suitable dimension. (Sometimes the zero matrices are scalar, sometimes they are row or column matrices, and sometimes they are square matrices.) It is also understood that either some or all of the D_i matrices, for $i = 1, 2, 3, \ldots, l$, or the matrix L may be absent from the matrix A'. We will assume that both the D_i matrices and the matrix L are present in A', since the other cases are just exceptions of this case.

Note that by the definition of the determinant of a matrix, and the fact that A' is similar to A, we have

$$\det(A') = \det(A) = \pm 1 \text{ and }, \det(A') = d_1 \cdot d_2 \cdot d_3 \cdot \ldots \cdot d_k, \text{ so}$$

$$\det(A') = d_1 \cdot d_2 \cdot d_3 \cdot \ldots \cdot d_{l-1} \cdot d_l \cdot d_{l+1} \cdot \ldots \cdot d_k = \pm 1,$$

and since we are in the field F, it follows that $d_i \neq 0$, for $i = 1, 2, 3, \ldots, k$.

Now if we divide the last column of each $D_i = \begin{bmatrix} 0 & d_i \\ I & B_i \end{bmatrix}$ matrix by $-d_i \neq 0$, we obtain the revised matrix $\begin{bmatrix} 0 & -1 \\ I & -\frac{1}{d_i}B_i \end{bmatrix}$, for $i = 1, 2, 3, \ldots, l$, and if we now move the last column of this revised matrix to the left of all the other columns and place it first, we obtain the new matrix D_i' defined by

$$D_i' = \begin{bmatrix} -1 & 0 \\ -\frac{1}{d_i}B_i & I \end{bmatrix}, \text{ for } i = 1, 2, 3, \ldots, l.$$

Also, if we take the matrix $L = \begin{bmatrix} d_{l+1} & 0 & 0 & \cdots & 0 \\ 0 & d_{l+2} & 0 & \cdots & 0 \\ 0 & 0 & d_{l+3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_k \end{bmatrix}$ and replace all the d_i non-zero diagonal entries, where $i = l+1, l+2, \ldots, k$, by 1's, we obtain the identity matrix I_{k-l}, and if we pair up and then interchange neighboring columns in this identity matrix, starting with the leftmost two columns, we end up with a revised form L' of the matrix L. This new matrix L' will either be of the form

$$L' = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}, \text{ if } k-l \text{ is even,}$$

or of the form

$$L' = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}, \text{ if } k-l \text{ is odd.}$$

Therefore, either L' is the direct sum of copies of the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, of size 2, or L' is the direct sum of copies of the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, of size 2, and the scalar matrix $[1]$, of size 1. Since this first form of L' is really just a special case of the second form of L', for sake of simplicity we will assume that L' is of the second form, that is, L' is the direct sum of copies of the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and the scalar matrix $[1]$.

Now if we consider the direct sum of the altered matrices

$$D_i' = \begin{bmatrix} -1 & 0 \\ -\frac{1}{d_i}B_i & I \end{bmatrix}, \text{ for } i = 1, 2, 3, \ldots, l,$$

and the altered matrix L', we obtain a new $n \times n$ matrix W where

$$W = D_1' \oplus D_2' \oplus D_3' \oplus \ldots \oplus D_l' \oplus L' =$$

$$\begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -\frac{1}{d_1}B_1 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{d_2}B_2 & I & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -\frac{1}{d_l}B_l & I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix},$$

where the 0's and I's denote the zero and identity matrices, respectively, of suitable dimension.

Since

$$W^2 = \begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -\frac{1}{d_1}B_1 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{d_2}B_2 & I & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -\frac{1}{d_l}B_l & I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} *$$

$$\begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -\frac{1}{d_1}B_1 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{d_2}B_2 & I & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -\frac{1}{d_l}B_l & I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix}
1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & I & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1
\end{bmatrix} = I_n,$$

then it follows that W is an involution in $\pm SL(n, F)$.

Define the weighted permutation matrix $R \in M(n, F)$ by

$$R = \begin{bmatrix}
0 & -d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & -d_2 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & I & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & -d_l & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{l+2} & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{l+1} & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & d_{l+4} & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_{l+3} & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & d_k
\end{bmatrix},$$

where the 0's and I's denote the zero and identity matrices, respectively, of suitable dimension.

Note that

$$\det(R) = \pm(d_1 \cdot d_2 \cdot d_3 \cdot \ldots \cdot d_{l-1} \cdot d_l \cdot d_{l+1} \cdot \ldots \cdot d_k) = \pm \det(A') = \pm(\pm 1) = \pm 1,$$

and so $R \in \pm SL(n, F)$.

Now

$$WR = \begin{bmatrix} -1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -\frac{1}{d_1}B_1 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{d_2}B_2 & I & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -\frac{1}{d_l}B_l & I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix} *$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & -d_2 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & -d_l & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{l+2} & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{l+1} & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & d_{l+4} & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_{l+3} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & d_k \end{bmatrix} =$$

$$\begin{bmatrix} 0 & d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ I & B_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & d_2 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & B_2 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & d_l & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & I & B_l & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{l+1} & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{l+2} & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_{l+3} & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & d_{l+4} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & d_k \end{bmatrix} = A',$$

and so at this point we know that A' can be written as the product of an involution W and a weighted permutation matrix R over F.

Denote by σ the permutation that corresponds to the weighted permutation matrix R. So

$\sigma = (1,2)(3,4)(5,6)\cdots(r-1,r)(r+1,r+2)\cdots(s-2,s-1)(s,s+1)(n)$, where $r < s$ and $r, s \in \{1,2,3,\ldots,n\}$,

and define the permutation τ in S_n by

$$\tau = (1)(2,3)(4,5)\cdots(r,r+1)(r+2,r+3)\cdots(s-1,s)(s+1,n).$$

Then

$$\tau\sigma = (1,3,5,7,\ldots,r-1,r+1,r+3,\ldots,s-2,s,n,s+1,s-1,\ldots,r+2,r,r-2,\ldots,6,4,2) = \rho,$$

which is a cycle on all n indices, and so τ ”ties together” the cycles in σ.

Now the permutation matrix corresponding to the permutation τ is the $n \times n$ matrix

$$X = \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 & 0 \\ 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 & 0 \\ 0 & 0 & 0 & I & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & I \\ 0 & 0 & 0 & 0 & 0 & \cdots & I & 0 \end{bmatrix} \text{ over } F.$$

Since we have

$$X^2 = \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 & 0 \\ 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 & 0 \\ 0 & 0 & 0 & I & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & I \\ 0 & 0 & 0 & 0 & 0 & \cdots & I & 0 \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 & 0 \\ 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 & 0 \\ 0 & 0 & 0 & I & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & I \\ 0 & 0 & 0 & 0 & 0 & \cdots & I & 0 \end{bmatrix} = I_n,$$

then it follows that X is an involution in $\pm SL(n,F)$.

Now define the $n \times n$ matrix $K \in M(n,F)$ by

$$K = XR = \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & I \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & I & 0 \end{bmatrix} *$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -d_2 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & d_{k-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & d_{k-4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{k-1} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{k-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_k \end{bmatrix} =$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -d_2 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & d_{k-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{k-1} & 0 \\ 0 & 0 & 0 & 0 & \cdots & d_{k-4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_k \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{k-2} & 0 & 0 \end{bmatrix},$$

and since $\det(K) = \det(XR) = \det(X)\det(R) = (\pm 1)(\pm 1) = (\pm 1)$, we have $K \in \pm SL(n, F)$, which means that K can be written as the product of some number of involutions over F. Also, since X is an involution, we have $XR = K \Rightarrow XXR = XK \Rightarrow R = XK$, and so A' becomes

$$A' = WR = WXK,$$

where W and X are both involutions in $\pm SL(n, F)$. Now, if we can now show that $K \in \pm SL(n, F)$ can be written as the product of exactly two involutions over F, then we have proven the statement of the theorem.

Consider the matrix $M \in M(n, F)$ defined by

$$M = [e_1, e_3, e_5, e_7, \ldots, e_{s-2}, e_s, (d_{k-2})e_n, (d_k d_{k-2})e_{s+1}, (d_k d_{k-1} d_{k-2})e_{s-1}, \ldots, (d_k d_{k-1} d_{k-2} \ldots (-d_5)(-d_4))e_6,$$

$$(d_k d_{k-1} d_{k-2} \ldots (-d_5)(-d_4)(-d_3))e_4, (d_k d_{k-1} d_{k-2} \ldots (-d_4)(-d_3)(-d_2))e_2],$$

where each e_i is $1 \times n$ and s is the same as in the permutations σ and τ. Let $\beta = (d_k d_{k-1} d_{k-2} \ldots (-d_5)(-d_4))$, let γ denote the coefficient $\beta(-d_3) = (d_k d_{k-1} d_{k-2} \ldots (-d_5)(-d_4)(-d_3))$ of e_4 in M, let δ denote the coefficient $\gamma(-d_2) = (d_k d_{k-1} d_{k-2} \ldots (-d_4)(-d_3)(-d_2))$ of e_6 in M, and let $\epsilon = \delta(-d_1) = (d_k d_{k-1} d_{k-2} \ldots (-d_4)(-d_3)(-d_2)(-d_1))$.

Then

$$M = \begin{bmatrix} I & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \delta \\ 0 & I & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & \gamma & 0 \\ 0 & 0 & I & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \iddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & d_{k-2} & \cdots & 0 & 0 \end{bmatrix}.$$

Now $\det(M)$ is a product in which each factor is some d_i, for $i \in \{1, 2, 3, \ldots, n\}$, and since earlier we noted that $d_i \neq 0$, for $i = 1, 2, 3, \ldots, k$, and we are in the field F, then it follows that $\det(M) \neq 0$. Since $\det(M) \neq 0$, then M is non-singular, so $M \in GL(n, F)$ and M^{-1} exists.

Define by $Q \in M(n, F)$ the matrix

$$Q = \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & \frac{1}{d_{k-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \frac{1}{\gamma} & 0 & \cdots & 0 \\ 0 & \frac{1}{\delta} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then

$$MQ = \begin{bmatrix} I & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & \delta \\ 0 & I & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & \gamma & 0 \\ 0 & 0 & I & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & d_{k-2} & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & \frac{1}{d_{k-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \frac{1}{\gamma} & 0 & \cdots & 0 \\ 0 & \frac{1}{\delta} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} =$$

$$\begin{bmatrix} I & 0 & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & 0 & \cdots & 0 \\ 0 & 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & I \end{bmatrix} = I_n,$$

and so Q is a right-inverse of M. Now since M is square, then any right-inverse of M is also a left-inverse, and so by the uniqueness of inverses we have $M^{-1} = Q$.

Let us now consider the product

$$M^{-1}KM = \begin{bmatrix} I & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & I & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & \frac{1}{d_{k-2}} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \frac{1}{\gamma} & 0 & \cdots & 0 \\ 0 & \frac{1}{\delta} & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} *$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -d_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -d_3 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & d_{k-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & d_{k-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & d_{k-4} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & d_k \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d_{k-2} & 0 & 0 \end{bmatrix} M =$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \frac{d_{k-2}}{d_{k-2}} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \frac{-d_3}{\gamma} & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-d_2}{\delta} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \end{bmatrix} M =$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & \frac{d_{k-2}}{d_{k-2}} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \frac{-d_3}{\beta(-d_3)} & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{-d_2}{\gamma(-d_2)} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \end{bmatrix} M =$$

$$\begin{bmatrix} 0 & -d_1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ I & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\beta} & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\gamma} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} I & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & \delta \\ 0 & I & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \gamma & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & \delta(-d_1) \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \frac{\gamma}{\gamma} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & \epsilon \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} = S \in M(n, F).$$

Since $\epsilon = d_k d_{k-1} d_{k-2} \dots (-d_4)(-d_3)(-d_2)(-d_1) = \pm \det(A') = \pm(\pm 1) = \pm 1$, then

$$S = \begin{bmatrix} 0 & 0 & \cdots & 0 & \pm 1 \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \in \pm SL(n, F).$$

Now

$$SS^T = \begin{bmatrix} 0 & 0 & \cdots & 0 & \pm 1 \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \pm 1 & 0 & 0 & \cdots & 0 \end{bmatrix} = I_n,$$

and since S^T is a right-inverse of S, then it is also a left-inverse, and since we are in a field it follows that $S^T = S^{-1}$. Now, by Note 9 in Section 2, we know that a square matrix over a field is similar to its transpose, and so we have that S is similar to $S^T = S^{-1}$.

Since S is similar to S^{-1}, then, by Theorem 2 in Section 4, we know that S can be written as a product of two involutions over F. Now K is similar to S, and so by Theorem 1 in Section 3 we know that K can also be written as the product of two involutions over F, say $K = YZ$, where $Y, Z \in \pm SL(n, F)$ are both involutions.

So now we have

$$A' = WR = WXK = WXYZ,$$

where $W, X, Y,$ and Z are all involutions in $\pm SL(n, F)$, and since we have shown that A' can be written as the product of four involutions over F, then, by similarity, so can the matrix A.

Therefore we have shown that any matrix in $\pm SL(n, F)$ can be written as the product of at most four involutions over F. ◇

The following example gives an illustration of the method used in the proof of Theorem 5.

Example 35. *(A Product of not More than Four Involutions)*

Let $A = \begin{bmatrix} 0 & -3 & 0 & 0 & 0 \\ 2 & -2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 5 & 0 \\ 0 & 0 & 5 & 4 & 0 \\ 0 & 0 & -3 & -3 & 1 \end{bmatrix} \in \pm SL(5, Z_{11})$. We will follow the construction of Theorem 5 to show that A can be written as the product of not more than four involutions (it might be the case that A can be written as the product of two or three involutions, however, in this example we are only concerned with showing that four involutions will suffice).

Define $B \in GL(5, Z11)$ by $B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 2 \end{bmatrix}$. Then $B^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & -5 & 5 & 0 \\ 0 & 0 & -5 & -5 & 0 \end{bmatrix}$.

Now

$$B^{-1}AB = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & -5 & 5 & 0 \\ 0 & 0 & -5 & -5 & 0 \end{bmatrix} \begin{bmatrix} 0 & -3 & 0 & 0 & 0 \\ 2 & -2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 5 & 0 \\ 0 & 0 & 5 & 4 & 0 \\ 0 & 0 & -3 & -3 & 1 \end{bmatrix} B =$$

$$\begin{bmatrix} 0 & -3 & 0 & 0 & 0 \\ 2 & -2 & 0 & 0 & 0 \\ 0 & 0 & 4 & 5 & 0 \\ 0 & 0 & 5 & 4 & 0 \\ 0 & 0 & -3 & -3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} = A'.$$

So the matrix A is similar to the matrix $A' = \begin{bmatrix} 0 & 5 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$, and also $A' = D_1 \oplus L$, where $L = D_2 \oplus D_3 \oplus D_4$, and D_1, D_2, D_3, and D_4 are the following companion matrices of irreducible polynomials over F:

$$D_1 = \begin{bmatrix} 0 & 5 \\ 1 & -2 \end{bmatrix}, D_2 = [1], D_3 = [-1], \text{ and } D_4 = [-2].$$

Let $X = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in M(5, Z_{11})$.

Then

$$X^2 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 4-4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5,$$

and so X is an involution.

Let $R = \begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} \in M(5, Z_{11})$.

Then

$$XR = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ -4 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 0 & 0 \\ 1 & 20 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 5 & 0 & 0 & 0 \\ 1 & 9 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 5 & 0 & 0 & 0 \\ 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} = A',$$

and so it follows that A' can be written as the product of an involution X and a weighted permutation matrix R.

Now let $Y = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \in M(5, Z_{11})$.

Then

$$Y^2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5,$$

and so Y is an involution.

Consider the product

$$YR = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix} = \begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = K \in M(5, Z_{11}).$$

Since Y is an involution then we have

$$YR = K \Rightarrow YYR = YK \Rightarrow R = YK, \text{ and}$$

$$A' = XR \Rightarrow A' = XYK.$$

Let $M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \in M(5, Z_{11})$. Then $\det(M) = -4 \neq 0$, so M is non-singular and M^{-1} exists and is defined by $M^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & -5 & 0 & 0 & 0 \end{bmatrix}$.

Also

$$M^{-1}KM = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & -5 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} M =$$

$$\begin{bmatrix} 0 & -5 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 5 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = S \in M(5, Z_{11}).$$

Now

$$SS^T = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = I_5,$$

so $S^T = S^{-1}$, and since, by Note 8, every $n \times n$ matrix over a field is similar to its transpose, then S is similar to $S^T = S^{-1}$, and so, by Theorem 2, S can be written as the product of two involutions over Z_{11}.

Now K is similar to S, and so, by Theorem 1, K can also be written as the product of two involutions over Z_{11}, say $K = CD$, where $C, D \in \pm SL(5, Z_{11})$. So we now have $A' = XYK$, and $K = CD$, where X, Y, C, and D are all involutions over Z_{11}, hence

$$A' = XYK \Rightarrow A' = XYCD,$$

and so we have shown that A' can be written as the product of at most four involutions over Z_{11}.

Since A is similar to A', then, by Theorem 1, A can also be written as the product of at most four involutions over Z_{11}, and so we have shown that in this example the construction used in the proof of Theorem 5 does indeed produce the correct result. ◇

Before we proceed to the next section, Section 6, and examine which matrices can be written as the product of exactly three involutory matrices, let us consider one more example of a matrix that is the product of not more that four involutions.

Example 36. *(A Product of not More than Four Involutions)*

Consider the matrix

$$M = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 1 & 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 2 & 0 \end{bmatrix} \in \pm SL(4, Z_5).$$

Since

$$M^2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 2 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & -2 & 0 \\ -1 & 0 & 0 & -2 \end{bmatrix} \neq I_4,$$

then clearly M is not an involution in $\pm SL(4, Z_5)$.

Now, by Theorem 5, we know that M can be written as the product of at most four involutions over Z_5, and, in fact $M = WXYZ$, where W, X, Y and Z are defined by

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 \end{bmatrix} \in \pm SL(4, Z_5),$$

where $W^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4,$

$$X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \pm SL(4, Z_5),$$

$$\text{where } X^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4,$$

$$Y = \begin{bmatrix} -1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \in \pm SL(4, Z_5),$$

$$\text{where } Y^2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4,$$

$$Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \pm SL(4, Z_5),$$

$$\text{where } Z^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4, \text{ and}$$

$$WXYZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & -2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} YZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & -1 & 0 \\ 0 & 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} Z$$

$$= \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 2 & 0 \end{bmatrix} = M.$$

So we have shown that the matrix $M \in \pm SL(4, Z_5)$, can be written as the product of four involutions over Z_5. Now it might be the case that M can be written as the product of two or three involutions over Z_5, but, as we have shown, at *most* four involutions are needed. ◇

At this point we should mention that the *Four Involutions Theorem* applies to all matrices in $\pm SL(n, F)$, but in the general linear group, $GL(n, F)$, the theorem applies only to those matrices with determinant ± 1, i.e., only to the elements of $GL(n, F)$ that are also elements of $\pm SL(n, F)$.

In Examples 34, 35, and 36, we saw matrices that can be written as the product of four involutions and, more specifically, in Example 34, we showed that four involutions are indeed necessary in some cases, since the matrix of that example was not itself an involution and could not be written as the product of two or three involutions. Also, we have developed theorems that let us determine when a matrix can be written as the product of exactly two involutions (when it is similar to its inverse), and we have proved the *Four Involutions Theorem* which states that any matrix of determinant ± 1 over a field F can be written as the product of at most ***four*** involutions. We should mention that there is no need to consider matrices that are the product of more than four involutions, since these matrices are in $\pm SL(n, F)$, as we have shown in Proposition 2 of Section 3, and so, by Theorem 5, they can be rewritten as the product of four involutory matrices over $\pm SL(n, F)$. The next logical question that we should consider is

> *Can we characterize the matrices of determinant ± 1 over a field F that can be written as the product of exactly three involutions?*

This question leads us to the next section, Section 6.

Section 6. Products of Three Involutions

In Section 4, Example 33, we gave an example of a matrix that cannot be written as a product of two involutions but that can be written as the product of exactly three involutions. The special property that this matrix possesses which enables us to use three involutions in its factorization instead of four (which, by Theorem 5, is the most that are needed in any case), is the fact that this matrix is cyclic. This observation leads is to the first theorem of this section.

Theorem 6 (cf. [2]). *If $A \in \pm SL(n, F)$ is a cyclic matrix, then A can be written as the product of exactly three involutions over F.*

Proof (Theorem 6).

Let $A \in \pm SL(n, F)$ be a cyclic matrix. Then A is similar to the companion matrix A' of an irreducible polynomial over F, and so if we can show that A' can be written as the product of exactly three involutions over F, then, by Theorem 1 in Section 3, so can A.

Since A' is the companion matrix of an irreducible polynomial over the field F, then A' is an $n \times n$ matrix of the form

$$A' = \begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha \\ 1 & 0 & \cdots & 0 & * \\ 0 & 1 & \cdots & 0 & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \end{bmatrix} = \begin{bmatrix} 0 & \alpha \\ I_{n-1} & B \end{bmatrix},$$

where 0 is the $1 \times (n-1)$ zero matrix, and B is an $(n-1) \times 1$ column matrix.

Now $\det(A) = \pm 1$ (since $A \in \pm SL(n, F)$), and since A' is similar to A, then it follows that

$$\det(A') = \det(A) = \pm 1.$$

However, since A' is a companion matrix of an irreducible polynomial over F, we also have

$$\det(A') = \alpha \cdot 1 \cdot 1 \cdot \ldots \cdot 1 = \alpha.$$

Since $\det(A') = \alpha$ and $\det(A') = \pm 1$, it follows that $\alpha = 1$ or $\alpha = -1$, and so, in any case

$$\alpha^2 = 1.$$

Define the matrix $J_n \in \pm SL(n, F)$ by

$$J_n = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then

$$J_n^2 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

and so it follows that J_n is an involution.

Now define $X \in M(n, F)$ by

$$X = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix}.$$

Then

$$X^2 = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix}\begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (\alpha B) + (-\alpha B) & I_{n-1} \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} = I_n,$$

and so X is an involution in $\pm SL(n, F)$.

Define the matrix $Y \in M(n, F)$ by

$$Y = \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix}.$$

Then

$$Y^2 = \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix}\begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix} = \begin{bmatrix} \alpha^2 & 0 \\ 0 & (J_{n-1})^2 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} = I_n,$$

and so Y is an involution in $\pm SL(n, F)$.

Finally, define the matrix $Z \in M(n, F)$ by

$$Z = \begin{bmatrix} 0 & 1 \\ J_{n-1} & 0 \end{bmatrix} = J_n.$$

Then Z is also an involution in $\pm SL(n, F)$.

Now

$$XYZ = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix}\begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix} Z = \begin{bmatrix} \alpha & 0 \\ \alpha^2 B & J_{n-1} \end{bmatrix} Z =$$
$$\begin{bmatrix} \alpha & 0 \\ B & J_{n-1} \end{bmatrix}\begin{bmatrix} 0 & 1 \\ J_{n-1} & 0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha \\ (J_{n-1})^2 & B \end{bmatrix} =$$
$$\begin{bmatrix} 0 & \alpha \\ I_{n-1} & B \end{bmatrix} = A',$$

and so we have shown that A' can be written as the product of exactly three involutory matrices over F, and so, by Theorem 1, since A is similar to A', so can A.

Thus if $A \in \pm SL(n, F)$ is a cyclic matrix, then A can be written as the product of exactly three involutions over F. ◇

Example 37. *(<u>A Cyclic Matrix that is the Product of Three Involutions</u>)*

Let $f(x) = x^3 + 4x + 1 \in Z_{11}[x]$. Then, since $f(x)$ has no zeros in Z_{11}, it follows that $f(x)$ is irreducible over Z_{11}, and the companion matrix $Com(f) \in M(3, Z_{11})$ of $f(x)$ is defined by

$$Com(f) = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{bmatrix}.$$

Let $A = \begin{bmatrix} -4 & 0 & -5 \\ -4 & 2 & 5 \\ 0 & -1 & 2 \end{bmatrix} \in \pm SL(3, Z_{11})$. Then there exists a matrix $B = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ -1 & -1 & -2 \end{bmatrix} \in GL(3, Z_{11})$, with $B^{-1} = \begin{bmatrix} -2 & -1 & -2 \\ 4 & 1 & 3 \\ -1 & 0 & -1 \end{bmatrix}$, such that

$$B^{-1}AB = \begin{bmatrix} -2 & -1 & -2 \\ 4 & 1 & 3 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} -4 & 0 & -5 \\ -4 & 2 & 5 \\ 0 & -1 & 2 \end{bmatrix} B = \begin{bmatrix} 1 & 0 & 1 \\ 2 & -1 & 2 \\ 4 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ -1 & 0 & 2 \\ -1 & -1 & -2 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{bmatrix} = Com(f).$$

So A is similar to the companion matrix of an irreducible polynomial over Z_{11}, i.e., A is cyclic, and so, by Theorem 6, we know that A can be written as the product of three involutions in $\pm SL(3, Z_{11})$. $\diamond$

Example 38. *(A Product of Three Involutions)*

Consider the companion matrix $Com(f) = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{bmatrix} \in M(3, Z_{11})$ of Example 37 and define the matrices X, Y, and Z in $M(3, Z_{11})$ by

$$X = \begin{bmatrix} -1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, Y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \text{ and } Z = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then $X^2 = I_3, Y^2 = I_3$, and $Z^2 = I_3$, so X, Y, and Z are all involutions, and

$$XYZ = \begin{bmatrix} -1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} Z = \begin{bmatrix} -1 & 0 & 0 \\ -4 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{bmatrix} = Com(f),$$

and so it follows that the companion matrix $Com(f)$ is indeed the product of three involutory matrices over Z_{11}. $\diamond$

The previous theorem gives a sufficient, but not necessary, condition for a matrix to be written as the product of exactly three involutions. The following theorem gives another such sufficient condition for a matrix to be factored as a product of three involutory matrices.

Theorem 7. *Let $A \in \pm SL(p, F)$ be similar to the direct sum of two cyclic matrices over F. Then A can be written as the product of exactly three involutions in $\pm SL(p, F)$.*

Proof (Theorem 7).

Let $A \in \pm SL(p, F)$ be similar to the direct sum of two cyclic matrices over F. Say A is similar to A', where $A' = A_1 \oplus A_2$, and $A_1 \in \pm SL(n, F)$ and $A_2 \in \pm SL(m, F)$ are both cyclic, with $n + m = p$.

So

$$A' = A_1 \oplus A_2 = \begin{bmatrix} A_1 & 0_{n\times m} \\ 0_{m\times n} & A_2 \end{bmatrix},$$

and by Theorem 6 we know that since $A_1 \in \pm SL(n,F)$ and $A_2 \in \pm SL(m,F)$ are both cyclic then each can be written as the product of three involutions over F.

Let

$$A_1 = KLM, \text{ where } K, L, \text{ and } M \in \pm SL(n,F) \text{ are all } n \times n \text{ involutions, and}$$

$$A_2 = XYZ, \text{ where } X, Y, \text{ and } Z \in \pm SL(m,F) \text{ are all } m \times m \text{ involutions.}$$

Then A' becomes

$$A' = A_1 \oplus A_2 = \begin{bmatrix} A_1 & 0_{n\times m} \\ 0_{m\times n} & A_2 \end{bmatrix} = \begin{bmatrix} KLM & 0_{n\times m} \\ 0_{m\times n} & XYZ \end{bmatrix}.$$

Define the matrices $B, C,$ and $D \in \pm SL(p,F)$ by $B = \begin{bmatrix} K & 0_{n\times m} \\ 0_{m\times n} & X \end{bmatrix}$, $C = \begin{bmatrix} L & 0_{n\times m} \\ 0_{m\times n} & Y \end{bmatrix}$, and $D = \begin{bmatrix} M & 0_{n\times m} \\ 0_{m\times n} & Z \end{bmatrix}$.

Then we have

$$B^2 = \begin{bmatrix} K & 0_{n\times m} \\ 0_{m\times n} & X \end{bmatrix}\begin{bmatrix} K & 0_{n\times m} \\ 0_{m\times n} & X \end{bmatrix} = \begin{bmatrix} K^2 & 0_{n\times n} \\ 0_{m\times m} & X^2 \end{bmatrix} = \begin{bmatrix} I_n & 0_n \\ 0_m & I_m \end{bmatrix} = I_p,$$

$$C^2 = \begin{bmatrix} L & 0_{n\times m} \\ 0_{m\times n} & Y \end{bmatrix}\begin{bmatrix} L & 0_{n\times m} \\ 0_{m\times n} & Y \end{bmatrix} = \begin{bmatrix} L^2 & 0_{n\times n} \\ 0_{m\times m} & Y^2 \end{bmatrix} = \begin{bmatrix} I_n & 0_n \\ 0_m & I_m \end{bmatrix} = I_p,$$

and

$$D^2 = \begin{bmatrix} M & 0_{n\times m} \\ 0_{m\times n} & Z \end{bmatrix}\begin{bmatrix} M & 0_{n\times m} \\ 0_{m\times n} & Z \end{bmatrix} = \begin{bmatrix} M^2 & 0_{n\times n} \\ 0_{m\times m} & Z^2 \end{bmatrix} = \begin{bmatrix} I_n & 0_n \\ 0_m & I_m \end{bmatrix} = I_p,$$

and so $B, C,$ and D are all involutions in $\pm SL(p,F)$.

Now

$$BCD = \begin{bmatrix} K & 0_{n\times m} \\ 0_{m\times n} & X \end{bmatrix}\begin{bmatrix} L & 0_{n\times m} \\ 0_{m\times n} & Y \end{bmatrix}\begin{bmatrix} M & 0_{n\times m} \\ 0_{m\times n} & Z \end{bmatrix} =$$

$$\begin{bmatrix} KL & 0_{n\times m} \\ 0_{m\times n} & XY \end{bmatrix}\begin{bmatrix} M & 0_{n\times m} \\ 0_{m\times n} & Z \end{bmatrix} = \begin{bmatrix} KLM & 0_{n\times m} \\ 0_{m\times n} & XYZ \end{bmatrix} =$$

$$\begin{bmatrix} A_1 & 0_{n\times m} \\ 0_{m\times n} & A_2 \end{bmatrix} = A'.$$

Since A' can be written as the product of three involutions in $\pm SL(p,F)$, then, by similarity and Theorem 1, so can the matrix A.

Hence if $A \in \pm SL(p,F)$ is similar to the direct sum of two cyclic matrices, then A can be written as the product of three involutory matrices over F. ◇

Example 39. *(A Product of Three Involutions)*

Let

$$A = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} B & 0_{2\times 3} \\ 0_{3\times 2} & C \end{bmatrix} = B \oplus C \in \pm SL(5, Z_7).$$

Now $B = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} \in \pm SL(2, Z_7)$, is the companion matrix of the irreducible polynomial $f(x) = x^2 - 2x + 1$ over Z_7, and $C = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix} \in \pm SL(3, Z_7)$, is the companion matrix of the irreducible polynomial $g(x) = x^3 + 2x + 1$ over Z_7.

If we follow the construction used in the proof of Theorem 6, there exist involutions X, Y, and Z in $\pm SL(2, Z_7)$, defined by

$$X = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix}, Y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ and } Z = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

such that

$$XYZ = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} Z = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix} = B,$$

and so it follows that B is the product of three involutions in $\pm SL(2, Z_7)$.

Also, there exist involutions L, M, and N in $\pm SL(3, Z_7)$, defined by

$$L = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \text{ and } N = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

such that

$$LMN = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} N = \begin{bmatrix} -1 & 0 & 0 \\ -2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & -2 \\ 0 & 1 & 0 \end{bmatrix} = C,$$

and so the matrix C is the product of three involutory matrices in $\pm SL(3, Z_7)$.

Define the matrices F, G, and H in $\pm SL(5, Z_7)$ by

$$F = \begin{bmatrix} X & 0_{2\times3} \\ 0_{3\times2} & L \end{bmatrix}, G = \begin{bmatrix} Y & 0_{2\times3} \\ 0_{3\times2} & M \end{bmatrix}, \text{ and } H = \begin{bmatrix} Z & 0_{2\times3} \\ 0_{3\times2} & N \end{bmatrix}.$$

Then

$$F^2 = \begin{bmatrix} X & 0_{2\times3} \\ 0_{3\times2} & L \end{bmatrix} \begin{bmatrix} X & 0_{2\times3} \\ 0_{3\times2} & L \end{bmatrix} = \begin{bmatrix} X^2 & 0_{2\times3} \\ 0_{3\times2} & L^2 \end{bmatrix} = \begin{bmatrix} I_2 & 0_2 \\ 0_3 & I_3 \end{bmatrix} = I_5,$$

$$G^2 = \begin{bmatrix} Y & 0_{2\times3} \\ 0_{3\times2} & M \end{bmatrix} \begin{bmatrix} Y & 0_{2\times3} \\ 0_{3\times2} & M \end{bmatrix} = \begin{bmatrix} Y^2 & 0_{2\times2} \\ 0_{3\times3} & M^2 \end{bmatrix} = \begin{bmatrix} I_2 & 0_2 \\ 0_3 & I_3 \end{bmatrix} = I_5,$$

and

$$H^2 = \begin{bmatrix} Z & 0_{2\times3} \\ 0_{3\times2} & N \end{bmatrix} \begin{bmatrix} Z & 0_{2\times3} \\ 0_{3\times2} & N \end{bmatrix} = \begin{bmatrix} Z^2 & 0_{2\times2} \\ 0_{3\times3} & N^2 \end{bmatrix} = \begin{bmatrix} I_2 & 0_2 \\ 0_3 & I_3 \end{bmatrix} = I_5,$$

and so F, H, and G are all involutions in $\pm SL(5, Z_7)$.

Now

$$FGH = \begin{bmatrix} X & 0_{2\times3} \\ 0_{3\times2} & L \end{bmatrix} \begin{bmatrix} Y & 0_{2\times3} \\ 0_{3\times2} & M \end{bmatrix} H = \begin{bmatrix} XY & 0_{2\times3} \\ 0_{3\times2} & LM \end{bmatrix} \begin{bmatrix} Z & 0_{2\times3} \\ 0_{3\times2} & N \end{bmatrix} =$$

$$\begin{bmatrix} XYZ & 0_{2\times 3} \\ 0_{3\times 2} & LMN \end{bmatrix} = \begin{bmatrix} B & 0_{2\times 3} \\ 0_{3\times 2} & C \end{bmatrix} = A,$$

and so A is the product of three involutions in $\stackrel{+}{-} SL(5, Z_7)$. $\diamond$

The last theorem of this section determines when scalar matrices over a field can be written as a product of three involutory factors.

Theorem 8 (cf. [3]). *Let $\alpha \in F$. Then the scalar matrix $\alpha I_n \in \stackrel{+}{-} SL(n, F)$ can be written as the product of three involutions over F, if either*

1) $\alpha^2 = 1$, or

2) n is even and $\alpha^2 = -1 \neq 1$.

Proof (Theorem 8).

Let $\alpha \in F$, and let $\alpha I_n \in \stackrel{+}{-} SL(n, F)$ be the scalar matrix defined by α.

If (1) holds then $\alpha^2 = 1$, and so we have

$$\alpha I_n \cdot \alpha I_n = \alpha^2 I_n = I_n,$$

and so αI_n is itself an involution in $\stackrel{+}{-} SL(n, F)$.

Now since αI_n is an involution then it can also be written as the product of three involutions involutions in $\stackrel{+}{-} SL(n, F)$. For example,

$$\alpha I_n = \alpha I_n J_n J_n,$$

where $J_n \in \stackrel{+}{-} SL(n, F)$ is the $n \times n$ involution defined by

$$J_n = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Hence if (1) holds, then αI_n can be written as the product of three involutions, and so in this case we are done.

Now if (2) holds, then n is even and $\alpha^2 = -1 \neq 1$.

Since n is even, then $n = 2k$ for some positive integer k, and so $\alpha I_n = \alpha I_{2k} = \begin{bmatrix} \alpha I_k & 0 \\ 0 & \alpha I_k \end{bmatrix}$, can be factored as

$$\alpha I_n = \alpha I_{2k} = \begin{bmatrix} \alpha I_k & 0 \\ 0 & \alpha I_k \end{bmatrix} = \begin{bmatrix} 0 & \alpha I_k \\ -\alpha I_k & 0 \end{bmatrix} \begin{bmatrix} -I_k & 0 \\ 0 & I_k \end{bmatrix} \begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix}.$$

Since

$$\begin{bmatrix} 0 & \alpha I_k \\ -\alpha I_k & 0 \end{bmatrix} \begin{bmatrix} -I_k & 0 \\ 0 & I_k \end{bmatrix} \begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha I_k \\ \alpha I_k & 0 \end{bmatrix} \begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix} = \begin{bmatrix} \alpha I_k & 0 \\ 0 & \alpha I_k \end{bmatrix} = \alpha I_{2k} = \alpha I_n.$$

Now

$$\begin{bmatrix} 0 & \alpha I_k \\ -\alpha I_k & 0 \end{bmatrix}\begin{bmatrix} 0 & \alpha I_k \\ -\alpha I_k & 0 \end{bmatrix} = \begin{bmatrix} -\alpha^2 I_k & 0 \\ 0 & -\alpha^2 I_k \end{bmatrix} = \begin{bmatrix} -(-1)I_k & 0 \\ 0 & -(-1)I_k \end{bmatrix} = \begin{bmatrix} I_k & 0 \\ 0 & I_k \end{bmatrix} = I_{2k} = I_n,$$

$$\begin{bmatrix} -I_k & 0 \\ 0 & I_k \end{bmatrix}\begin{bmatrix} -I_k & 0 \\ 0 & I_k \end{bmatrix} = \begin{bmatrix} I_k & 0 \\ 0 & I_k \end{bmatrix} = I_{2k} = I_n, \text{ and}$$

$$\begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix}\begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix} = \begin{bmatrix} I_k & 0 \\ 0 & I_k \end{bmatrix} = I_{2k} = I_n,$$

so all of the matrices in the above factorization of αI_n are involutions in $\pm SL(n, F)$, and so, in this case, αI_n can be written as the product of three involutions over F.

Hence if either (1) or (2) in the statement of Theorem 8 hold, then αI_n can be written as the product of three involutions in $\pm SL(n, F)$. ◇

Example 40. *(A Scalar Matrix that is the Product of Three Involutions)*

Let $A = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} \in \pm SL(4, Z_{17})$. Then, since $4^2 = 16 = -1 \neq 1$, by Theorem 8, A can be written as the product of exactly three involutions in $\pm SL(4, Z_{17})$.

Now $X = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \end{bmatrix} \in \pm SL(4, Z_{17})$, is an involution since

$$X^2 = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -16 & 0 & 0 & 0 \\ 0 & -16 & 0 & 0 \\ 0 & 0 & -16 & 0 \\ 0 & 0 & 0 & -16 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4,$$

$Y = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \pm SL(4, Z_{17})$, is an involution since

$$Y^2 = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4, \text{ and}$$

$Z = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \in \pm SL(4, Z_{17})$, is an involution since

$$Z^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4.$$

Also

$$XYZ = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} Z = \begin{bmatrix} 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ -4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = A,$$

and so we have shown that A can be written as the product of three involutions $X, Y,$ and Z over Z_{17}. ◇

So far, in Theorems 6, 7, and 8 of this section, we have given various conditions for when a matrix over a field can be written as a product of three involutions. These conditions, however, are only sufficient; they are not necessary, since there may exist a matrix over a field that does not meet any of the conditions given in Theorems 6, 7, and 8, but that can still be written as a product of three involutions. As it turns out, the characterization of all the matrices over fields that can be written as a product of three involutions is not complete, and only certain special subsets of the set of all matrices that can be factored as a product of exactly three involutory matrices have been characterized.

Before we end this section and our discussion of products of involutions over fields and move on to the next section, Section 7, there is one last result from Ballantine [3] which we will present, but not prove, that further characterizes matrices over a field that can be written as a product of exactly three involutions.

Proposition 5 (cf. [3]). *A matrix $A \in \pm SL(n, F)$ can be written as the product of three involutions over F if and only if at least one of the following hold:*

a) $n \leq 2$,

b) F has order $2, 3,$ or 5,

c) $n = 3$ and either the characteristic of F is 3 or $f(x) = x^2 + x + 1$ is irreducible over F, or

d) $n = 4$ and the characteristic of F is 2. ◇

At this point we have completed our discussion of products of involutions over fields. In the next section, Section 7, we will deal with generalizing this concept of factoring a matrix as a product of special matrices to rings of special types that are not fields.

Section 7. Special Products Over Other Rings that are not Fields

In the previous sections we have studied square matrices over fields that can be written as the product of involutions. In this section we will extend this concept of factoring matrices into a product of special factors over specific types of commutative rings with unity. To this end, we are giving the following theorems, Theorem 9 and Theorem 10, without proof, since they provide us with rings that give rise to special factorizations of matrices.

Theorem 9 (cf. [19]). *Let A be a ring with unity such that A satisfies the first Bass stable range condition. Then every matrix in $GL(n, A)$, the group of all invertible $n \times n$ matrices with entries in the ring A, can be written as the product of two cyclic matrices in $GL(n, A)$.* $\diamond$

Theorem 10 (cf. [19]). *Let A be a ring with unity such that A satisfies the first Bass stable range condition. Then for any matrix in $M \in GL(n, A)$, and any companion matrix $S \in GL(n, A)$, there exist cyclic matrices L and K in $GL(n, A)$, such that $M = LK$, where L is similar to the given companion matrix S.* $\diamond$

Suppose now that there exist commutative rings with unity satisfying the first Bass stable range condition, and let R be such a ring. Then, by Theorem 9 and Theorem 10, we know that every element in $GL(n, R)$, the general linear group of all invertible matrices with entries over R, can be written as a product of two cyclic matrices in $GL(n, R)$, and, in fact, we have seen that we can further specify that the first factor in this product be a cyclic matrix that is similar to some given invertible companion matrix in $GL(n, R)$. The next theorem of this section considers products of involutions in such rings.

Theorem 11. *Let R be a commutative ring with unity. Then every cyclic matrix $A \in GL(n, A)$ with* $\det(A) = \pm 1$ *can be written as a product of three involutions over R.*

Proof (Theorem 11).

Let R be a commutative ring with unity, and let $A \in GL(n, R)$ be a cyclic matrix with $\det(A) = \pm 1$.

Since A is cyclic, then A is similar to the $n \times n$ companion matrix A' of an irreducible polynomial over R of the form

$$A' = \begin{bmatrix} 0 & 0 & \cdots & 0 & \alpha \\ 1 & 0 & \cdots & 0 & * \\ 0 & 1 & \cdots & 0 & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & * \end{bmatrix} = \begin{bmatrix} 0 & \alpha \\ I_{n-1} & B \end{bmatrix},$$

where 0 is the $1 \times (n-1)$ zero matrix, and B is an $(n-1) \times 1$ column matrix.

Now $\det(A) = \pm 1$ (since $A \in \pm SL(n, R)$), and since A' is similar to A, then it follows that

$$\det(A') = \det(A) = \pm 1.$$

However, since A' is a companion matrix of an irreducible polynomial over R, we also have

$$\det(A') = \alpha \cdot 1 \cdot 1 \cdot \ldots \cdot 1 = \alpha.$$

Since $\det(A') = \alpha$ and $\det(A') = \pm 1$, it follows that $\alpha = 1$ or $\alpha = -1$, and so, in any case

$$\alpha^2 = 1.$$

Define the matrix $J_n \in GL(n, R)$ by

$$J_n = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then

$$J_n^2 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \end{bmatrix},$$

and so it follows that J_n is an involution.

Now define $X \in M(n, R)$ by

$$X = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix}.$$

Then

$$X^2 = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix} \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ (\alpha B) + (-\alpha B) & I_{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} = I_n,$$

and so X is an involution in $GL(n, R)$.

Define the matrix $Y \in M(n, R)$ by

$$Y = \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix}.$$

Then

$$Y^2 = \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix} \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix} = \begin{bmatrix} \alpha^2 & 0 \\ 0 & (J_{n-1})^2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & I_{n-1} \end{bmatrix} = I_n,$$

and so Y is an involution in $GL(n, R)$.

Finally define the matrix $Z \in M(n, R)$ by

$$Z = \begin{bmatrix} 0 & 1 \\ J_{n-1} & 0 \end{bmatrix} = J_n.$$

Then Z is also an involution in $GL(n, R)$.

Now

$$XYZ = \begin{bmatrix} -1 & 0 \\ -\alpha B & I_{n-1} \end{bmatrix} \begin{bmatrix} -\alpha & 0 \\ 0 & J_{n-1} \end{bmatrix} Z = \begin{bmatrix} \alpha & 0 \\ \alpha^2 B & J_{n-1} \end{bmatrix} Z =$$

$$\begin{bmatrix}\alpha & 0\\ B & J_{n-1}\end{bmatrix}\begin{bmatrix}0 & 1\\ J_{n-1} & 0\end{bmatrix}=\begin{bmatrix}0 & \alpha\\ (J_{n-1})^2 & B\end{bmatrix}=$$
$$\begin{bmatrix}0 & \alpha\\ I_{n-1} & B\end{bmatrix}=A',$$

and so we have shown that A' can be written as the product of exactly three involutory matrices over R, and so, by Theorem 1, since A is similar to A', so can A.

Hence if $A \in GL(n,R)$ is a cyclic matrix with $\det(A) = \pm 1$, then A can be written as the product of exactly three involutions over R. ◇

So if R is a commutative ring with unity satisfying the first Bass stable range condition, then, by Theorems 9 and 10, we can factor any matrix in $GL(n,R)$ as the product of two cyclic matrices, the first of which is similar to a prescribed companion matrix S in $GL(n,R)$, say with $\det(S) = \pm 1$, and so now, by Theorem 11, since S is cyclic with determinant ± 1, then we can replace it with its factorization as a product of three involutions over R. This observation leads us to the final result of this section, Theorem 12.

Theorem 12. *Let R be a commutative ring with unity that satisfies the first Bass stable range condition, and let A be any matrix in $GL(n,A)$. Then A can be written as the product of three involutory matrices over R and a cyclic matrix C in $GL(n,R)$. Furthermore if $\det(C) = \pm 1$, then A can be written as the product of at most six involutory matrices over R.*

Proof (Theorem 12).

Let R be a commutative ring with unity satisfying the first Bass stable range condition, and let $A \in GL(n,R)$. Also let $S \in GL(n,R)$ be a companion matrix with $\det(S) = \pm 1$.

Then, by Theorem 9 and Theorem 10, we know that $A = BC$, where B and C are both cyclic matrices in $GL(n,R)$, and B is similar to the specified companion matrix S. Now since B is similar to S, then $\det(B) = \det(S) = \pm 1$, and since B is cyclic, by Theorem 11, B can be written as the product of three involutions in $GL(n,R)$, say $B = XYZ$, where X, Y, and Z are in $GL(n,R)$.

Hence

$$A = BC \Rightarrow A = XYZC,$$

where X, Y, and Z are all involutions in $GL(n,R)$, and C is a cyclic matrix in $GL(n,R)$.

Furthermore if $\det(C) = \pm 1$, then since C is cyclic, by Theorem 11, C can also be written as the product of three involutions in $GL(n,R)$, say $C = KLM$, where K, L, and M are in $GL(n,R)$.

So

$$A = BC \Rightarrow A = XYZKLM,$$

where X, Y, Z, K, L, and M are all involutions in $GL(n,R)$, and so in this case A can be written as the product of most six involutory matrices over R. ◇

Section 8. Summary

In the introduction, Section 1, we stated the following question which was to be the main topic of this paper:

> *Does there exist a smallest integer k, such that given any matrix $A \in \pm SL(n, F)$ which is a product of involutions, A can be written as the product of at most k involutions, and, if such an integer exists, what is it?*

The answer to this question, as we proved in Section 5 with the *Four Involutions Theorem*, is, of course, $k = 4$.

In Section 4 we considered which matrices, if any, can be written as the product of exactly two involutions, and we found that these matrices must be similar to their inverses, and that, in fact, the converse is also true. That is, if a matrix is similar to its inverse then it can be factored as the product of two involutory matrices. In Section 6 we considered the case of matrices that can be written as the product of exactly three involutory factors, and we saw that these matrices have not, as yet, been completely classified. Finally, in Section 7, we extended this concept of factoring a matrix into a product of special matrices to rings that were not fields, and we saw that if the ring was commutative with unity satisfying the first Bass stable range condition, then any matrix with entries over the ring can be factored into the product of two cyclic matrices.

As it turns out, this concept of taking a class of objects (in our case invertible matrices with a determinant of ± 1 over a field), studying products of elements from this class, and trying to find the minimal number of special factors (in our case involutions) required in a given factorization, is a frequently addressed topic. Other cases that have been, or are currently being studied by others, include products of normal matrices, of symmetric matrices, of elementary matrices, over various rings, fields, infinite-dimensional vector spaces, and Hilbert spaces.

Bibliography

[1] Agnew, J. L., and Knapp, R. C., *Linear Algebra with Applications* , Brooks-Cole, California, 1989.

[2] Ballantine, C. S., Some involutory similarities, *Linear and Multilinear Algebra* , 3 (1975), 19-23.

[3] Ballantine, C. S., Products of involutory matrices I, *Linear and Multilinear Algebra,* 5 (1977), 53-62.

[4] Beachy, J. A., and Blair, W.D., *Abstract Algebra with a Concrete Introduction*, Prentice-Hall, New Jersey, 1990.

[5] Brown, W. C., *Matrices Over Commutative Rings*, Marcel-Dekker, New York, 1993.

[6] Burden, R. L., and Faires, J. D., *Numerical Analysis*, PWS- Kent, New York, 1989.

[7] Curtis, C. W., *Linear Algebra, an Introductory Approach*, Springer-Verlag, New York, 1984.

[8] Fraleigh, J. B., *A First Course in Abstract Algebra*, Addison-Wesley, New York, 1989.

[9] Gustafson, W. H., Halmos, P. R., and Radjavi, H., Products of involutions, *Linear Algebra and Applications*, 13 (1976), 157-162.

[10] Gustafson, W. H., On Products of involutions, in *Paul Halmos Celebrating 50 Years of Mathematics*, Springer-Verlag, New York, 1991.

[11] Herstein, I. N., and Winter, D. J., *Matrix Theory and Linear Algebra*, Macmillan, New York, 1988.

[12] Hohn, F. E., *Elementary Matrix Algebra*, Macmillan, New York, 1973.

[13] Hungerford, T. W., *Algebra*, Springer-Verlag, New York, 1974.

[14] Lancaster, P., and Tismenetsky, M., *The Theory of Matrices*, Academic Press, New York, 1985.

[15] MacLane, S., and Birkhoff, G., *Algebra*, Macmillan, New York, 1967.

[16] Ortega, J. M., *Matrix Theory, a Second Course*, Plenum Press, New York, 1987.

[17] Spindler, K. H., *Abstract Algebra with Applications in Two Volumes, Volume I*, Marcel-Dekker, New York, 1994.

[18] Stewart, I., *Galois Theory*, Chapman and Hall, London, 1989.

[19] Vaserstein, L. N., and Wheland, E., Commutators and companion matrices over rings of stable rank 1, *Linear Algebra and its Applications* , 142 (1990), 263-277.