Chapter 5

Theory of Matrices

As before, $\mathbb{F}$ is a field. We use $\mathbb{F}[x]$ to represent the set of all polynomials of x with coefficients in $\mathbb{F}$. We use $M_{m,n}(\mathbb{F})$ and $M_{m,n}(\mathbb{F}[x])$ to denoted the set of m by n matrices with entries in $\mathbb{F}$ and $\mathbb{F}[x]$ respectively. When $m = n$, we write $M_{m,n}$ as M_n.

In this chapter we shall study seven RST (Reflective, Symmetric, Transitive) relations among matrices over $\mathbb{F}$:

1. **Equivalence over** $\mathbb{F}$: $B = PAQ$, where P and Q are invertible matrices over $\mathbb{F}$;
2. **Equivalence over** $\mathbb{F}[x]$: $B = PAQ$, where P and Q are invertible matrices over $\mathbb{F}[x]$;
3. **Congruence:** $B = P^T AP$, where P is invertible;
4. **Hermitian congruence:** $B = P^* AP$, where $\mathbb{F} = \mathbb{C}$ and $P^* := \bar{P}^T$ and is invertible;
5. **Similarity:** $B = P^{-1}AP$;
6. **Orthogonal similarity:** $B = P^{-1}AP$, where $\mathbb{F} = \mathbb{R}$ and $P^{-1} = P^T$;
7. **Unitary similarity:** $B = P^{-1}AP$, where $\mathbb{F} = \mathbb{C}$ and $P^{-1} = P^*$.

All of the relations except the first two require the related matrices A and B to be square. Otherwise the products defining the relations are impossible.

The seven relations are in three categories: **equivalent, congruent**, and **similar**. For each of the seven relations there are two major problems:

(1) *Obtaining a set of canonical matrices;*

(2) *Finding a necessary and sufficient condition for two matrices to obey the relation.*

Equivalence over $\mathbb{F}$ originates from solving system of linear equations, by making change of variables and performing operations on equations. Equivalence over $\mathbb{F}[x]$ is primarily a tool for the study of similarity and the system of linear constant coefficient ordinary differential equations.

Similarity occurs in the determination of all matrices representing a common linear transformation, or alternatively, in finding basis such that a linear transformation has a simple form.

Congruence originates from non-singular linear substitution in quadratic forms and Hermitian forms. It can be used to characterize quadratic surfaces.

Finally, if the linear substitution is required to preserve the length, congruence then becomes orthogonal or unitary similarity.

5.1 RST Relation

Definition 5.1. *Let S be a set. A* **relation** *on S is a collection R of ordered pairs from $S \times S$. We say x relates y and write $x \sim y$ if $(x, y) \in R$. We say x does not relate y and write $x \not\sim y$ if $(x, y) \notin R$.*

A relation is called **reflexive** *if $x \sim x$ for all $x \in S$;*

A relation is called **symmetric** *if $x \sim y$ implies $y \sim x$;*

A relation is called **transitive** *if $x \sim y$ and $y \sim z$ implies $x \sim z$;*

An **RST relation**[1] *is a reflexive, symmetric, and transitive relation.*

Given an RST relation $\sim$ on S, for each $x \in S$, the set $[\![x]\!] := \{y \in S \mid y \sim x\}$ is called the **equivalent class** *of x.*

Gives an RST relation, there are two fundamental problems:

1. finding a set of canonical forms, i.e., a set containing one and exactly one representative from each equivalent class.
2. finding convenient criteria to determine whether any given two elements are related or to find the canonical form which an arbitrarily given element relates.

Example 5.1. Consider $\mathbb{Z}$, the set of all integers. We define a "$mod(3)$" relation by

$$m \sim n \text{ if } m - n \text{ is an integer muptiple of 3.}$$

This is an RST relation which divides $\mathbb{Z}$ is into three equivalent classes:

$$Z_0 := \{3k \mid k \in \mathbb{Z}\}, \qquad Z_1 := \{1 + 3k \mid k \in \mathbb{Z}\}, \qquad Z_2 := \{2 + 3k \mid k \in \mathbb{Z}\}.$$

From each class, we pick-up one and only one representative, say 0 from Z_0, 1 from Z_1, and -1 from Z_2. Then we obtain a set $C = \{0, 1, -1\}$ of canonical forms. Each integer relates exactly one canonical form.

Criteria: An integer of the form $a_1 \cdots a_k$ (in dicimal) relates the remainder of $(a_1 + \cdots + a_k)/3$. For example: $n = 8230609$. Then the remainder of $(8 + 2 + 3 + 6 + 9)/3$ is 2, so $n \in Z_2$.

Exercise 1. *Let $S = M_n(\mathbb{F})$, the set of all square matrices of rank n and entries in $\mathbb{F}$. Which kind of relations (reflexive, symmetric, transitive, and/or RST) are the following?*

1. *$A \sim B$ if and only if $B = 0I$; e.g. $R = \{(A, 0I) \mid A \in S\}$;*
2. *$A \sim B$ if and only if $A = 0I$; e.g. $R = \{(0I, B) \mid B \in S\}$;*
3. *$A \sim B$ if and only if $A = B$; e.g. $R = \{(A, A) \mid A \in S\}$;*
4. *$A \sim B$ for all A and B; e.g. $R = \{(A, B) \mid A, B \in S\}$;*
5. *$A \sim B$ if and only if both A and B are invertible;*
6. *$A \sim B$ if and only if $A - B$ has at least one row of zeros;*
7. *$A \sim B$ if and only if $AB = 0I$.*

[1] This is commonly called "equivalence relation", but in this chapter such terminology would be confusing.

Exercise 2. *Demonstrate by examples that the three relations, reflexive, symmetric, and transitive, are independent to each other; namely, find examples of relations that satisfy (i) non of them, (ii) only one of them, (iii) only two of them, and (iii) all three of them.*

Exercise 3. *Suppose $\sim$ is an RST relation on a set S. Show that for every $x, y \in S$, either $[\![x]\!] = [\![y]\!]$ or $[\![x]\!] \cap [\![y]\!] = \emptyset$.*

5.2 Equivalence over F

Consider a linear system

$$\sum_{j=1}^{n} a^i_j x^j = b^i, \qquad i = 1, \cdots, m \tag{5.1}$$

of m equations and n unknowns $x_1, \cdots, x_n$. Here a^i_j, b^i are given numbers (scalars) in $\mathbb{F}$. This system can be put in a matrix form

$$A\mathbf{x} = \mathbf{b}, \quad A = (a^i_j)_{m\times n}, \quad \mathbf{x} = (x^j)_{n\times 1}, \quad \mathbf{b} = (b^i)_{m\times 1}\ .$$

In this form, the system may be regarded as having only one unknown, the vector $\mathbf{x}$.

Two systems of m-linear equations in n unknowns $x_1, \cdots, x_n$ are called **equivalent** if every solution of one system is also a solution of the other, and vice versa. Certain simple operations are commonly used to convert a system to an equivalent one that may be easier to solve. For instance, it surely makes no difference when an equation is written first or last or in some intermediate position.

An **elementary operation for a system of equations** is one of the following three types:

1. *Interchange two equations;*
2. *multiplication of an equation by an invertible scalar;*
3. *Addition to an equation by a scalar multiple of a different equation.*

A system of equations $A\mathbf{x} = \mathbf{b}$ can be recorded by an **augmented matrix**

$$G = (A\ \mathbf{b}).$$

The elementary operations of equations correspond to the elementary row operations (defined below) on the augmented matrix.

Definition 5.2. 1. *An* **elementary row operation** *is one of the followings:*

   (a) $\mathcal{O}_{ij}$*: Interchange the* i*th and* j*th rows;*

   (b) $\mathcal{O}_i(d)$ *: Multiplication of the* i*th row by an invertible scalar* d*;*

   (c) $\mathcal{O}_{ij}(c)$*: Addition to the* i*th row by a scalar* c *multiple of the* j*th row,* $i \neq j$*.*

2. *An* **elementary matrix** *is a matrix obtained by performing an elementary row operation on an identity matrix* I*. There are three types of elementary matrices:* E_{ij}*,* $E_i(d)$ *(*d *invertible), and* $E_{ij}(c)$*, obtained by performing* $\mathcal{O}_{ij}, \mathcal{O}_i(d)$*, and* $\mathcal{O}_{ij}(c)$ *on the identity matrix* I*, respectively.*

3. *A matrix is called in a* **Row-Reduced-Echelon-Form**[2] *or* **RREF***, if*

   (a) *every nontrivial row has 1 as its first non-zero entry, called a* **leading one***;*

   (b) *any leading one in a lower row occurs only to the right of its counterpart above it;*

   (c) *In any column containing a leading one, all entries above and below the leading one are zero;*

   (d) *all rows consisting entirely zeros, if any, occurs at the bottom of the matrix.*

4. *The* **row space** *of a matrix is the space spanned by all the row vectors of the matrix.*

[2] If $\mathbb{F}$ is not a field, say $\mathbb{F} = \mathbb{Z}$, the definition of RREF should be revised.

5. *Two matrices are called* **row equivalent** *if they have the same row spaces.*

6. *The row rank of a matrix is the dimension of the row space of the matrix.*

Lemma 5.1. *1. Every elementary matrix has an inverse, which is also elementary.*

2. *To perform an elementary row operation $\mathcal{O}$ on an $m \times n$ matrix A, calculate the product EA, where E is the matrix obtained by performing $\mathcal{O}$ on I_m, the identity matrix of rank m.*

3. *The row space of a matrix $B \in M_{r,n}(\mathbb{F})$ is a subspace of that of $A \in M_{m,n}(\mathbb{F})$ if and only if $B = PA$ for some $P \in M_{r,m}(\mathbb{F})$.*

Proof of 3. Write

$$A = \begin{pmatrix} \mathbf{a}^1 \\ \vdots \\ \mathbf{a}^m \end{pmatrix}, \qquad B = \begin{pmatrix} \mathbf{b}^1 \\ \vdots \\ \mathbf{b}^r \end{pmatrix}.$$

Then

$$\text{row space of } A = \text{span}\{\mathbf{a}^1, \cdots, \mathbf{a}^m\};$$
$$\text{row space of } B = \text{span}\{\mathbf{b}^1, \cdots, \mathbf{b}^r\}.$$

Hence, the row space of B is a subspace of the row space of A if and only if there exist scalars $p^i_j, i = 1, \cdots, r, j = 1, \cdots, m$ such that

$$\mathbf{b}^i = \sum_{j=1}^{m} p^i_j \mathbf{a}^j \quad \forall\, i = 1, \cdots, r;$$

namely, $B = PA$ where $P = (p^i_j)_{r \times m}$. □

By using the Gauss elimination process, one can prove the following:

Lemma 5.2. *1. Any matrix over a field can be transformed by elementary row operations to an RREF, which is unique. In particular, if the matrix is invertible, its RREF is the identity matrix.*

2. *Two matrices $A, B \in M_{m,n}(\mathbb{F})$ are row equivalent if and only if $B = PA$ for some invertible $P \in M_m(\mathbb{F})$; that is, A and B have the same row space.*

3. *A square matrix is invertible if and only if it is row equivalent to an identity matrix, if and only if it is a product of elementary matrices, and also if and only if its row vectors form a basis of $\mathbb{F}^n$.*

4. *If a matrix A is reduced to an identity matrix by a succession of elementary row operations, the same succession of row operation performed on the identity matrix produces A^{-1}:*

$$(A \;\; I) \quad \longrightarrow \quad (I \;\; A^{-1}).$$

Proof of 4. Suppose $\{\mathcal{O}_1, \cdots, \mathcal{O}_k\}$ is a succession of elementary row operations that transform A to I, then $I = E_k \dots E_1 A$ where each E_i is the matrix obtained by performing $\mathcal{O}_i$ on the identity matrix I. Hence, $A^{-1} = E_k \cdots E_1 = E_k \cdots E_1 I$; that is A^{-1} can be obtained by performing successively the row operations $\mathcal{O}_1, \cdots, \mathcal{O}_k$ on I. □

Corollary 5.1. *A system of simultaneous linear equations $A\mathbf{x} = \mathbf{b}$ has a solution $\mathbf{x}$ if and only if the rank of the augmented matrix $(A \;\; \mathbf{b})$ equals the rank of the coefficient matrix A.*

Analogous to the elementary operation on equations, we can perform elementary operation on variables $x_1, \cdots, x_n$; In particular, if we make a change of variable $\mathbf{y} = Q\mathbf{x}$ where $Q \in M_n(\mathbb{F})$ is invertible, then the system $A\mathbf{x} = \mathbf{b}$ is equivalent to $AQ\mathbf{y} = \mathbf{b}$.

Note that in recording the coefficient matrix of systems of linear equation, elementary operations on variables corresponding to column operations.

The **column space** of a matrix over a field is the space generated by all the column vectors of the matrix. The **column rank** of a matrix is the dimension of the column space of the matrix. Two matrices of same size are called **column equivalent** if they have the same column space.

The **elementary column operations** are the interchange of two columns, the multiplication of a column by an invertible scalar, and the addition to one column by a scalar multiple of a different column.

It is easy to show the following:

Lemma 5.3. *(i) Each elementary column operation on an $m \times n$ matrix can be achieved by multiplying the matrix from the right by an elementary matrix obtained by performing the same operation on I_n.*

(ii) Elementary column operations do not change the column space of matrices.

(iii) The column space of a matrix $B \in M_{m,r}(\mathbb{F})$ is a subspace of that of a matrix $A \in M_{m,n}(\mathbb{F})$ if and only if $B = AQ$ for some $Q \in M_{n,r}(\mathbb{F})$.

(iv) Two matrices A and B are column equivalent if and only if $B = AQ$ for some invertible Q.

(v) If a succession of elementary column operations transforms A to I, then the same succession of column operations transforms I to A^{-1}:

$$\begin{pmatrix} A \\ I \end{pmatrix} \longrightarrow \begin{pmatrix} I \\ A^{-1} \end{pmatrix}$$

Definition 5.3. *Two matrices A, B of same size are called* **equivalent** *over $\mathbb{F}$ if $B = PAQ$ where both P and Q are invertible matrices over $\mathbb{F}$.*

Note that if $A, B \in M_{m,n}(\mathbb{F})$, then $P \in M_m(\mathbb{F})$ and $Q \in M_n(\mathbb{F})$.

Equivalence is but one of many RST relations to be studied in this chapter. The following theorem provides answers for the basic questions regarding the equivalence relation:

1) What is the necessary and sufficient condition for two matrices to be equivalent?

2) What are the canonical forms?

Theorem 5.1. *1. Every matrix $A \in M_{m,n}(\mathbb{F})$ is equivalent to a matrix in which for some integer $r \geq 0$, the first r elements on the diagonal are 1 and all other elements of the matrix are 0, namely,*

$$A \sim \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},$$

where I_r is the identity matrix of rank r.

2. For any matrix over a field, its row rank is the same as its column rank, and is hence called the rank of the matrix.

3. Two matrices of same size over a field are equivalent if and only if they have the same rank.

4. Let $A \in M_{m,n}(\mathbb{F})$. Suppose a succession of elementary operations on the first m rows and n columns gives

$$\begin{pmatrix} A & I_m \\ I_n & \end{pmatrix} \longrightarrow \begin{pmatrix} D & P \\ Q & \end{pmatrix}.$$

Then $D = PAQ$.

Two applications of the above theorem can be found in the exercise. For convenience, we use the following definition:

Definition 5.4. *Let $\mathbf{A} : U \to V$ be a linear map from vector space U to vector space V, $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ a basis of U, and $\{\mathbf{v}_1, \cdots, \mathbf{v}_m\}$ a basis of V. Suppose $A \in M_{m,n}(\mathbb{F})$ is a matrix such that*

$$\mathbf{A}(\mathbf{u}_1 \ \cdots \ \mathbf{u}_n) := (\mathbf{A}\mathbf{u}_1 \ \cdots \mathbf{A}\mathbf{u}_m) = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_m)A.$$

Then, A is called the matrix of $\mathbf{A}$ under the basis $\{\mathbf{u}_1, \cdots, \mathbf{u}_m\}$ (of the definition domain) and the basis $\{\mathbf{v}_1, \cdots, \mathbf{u}_n\}$ (of the image domain).

Exercise 4. *Show that the RREF of a matrix is unique.*

Exercise 5. *Find matrices P_1, P and Q such that $P_1 A$ is an RREF and PAQ is in its canonical form, where A is one of the followings:*

$$\begin{pmatrix} 1 & 1 & 0 \\ 2 & 3 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Exercise 6. *If $x_1, \cdots, x_m$ and $y^1, \cdots, y^n$ are two sets of variables, a quadratic polynomial of the type*

$$q = \sum_{i=1}^{m} \sum_{j=1}^{n} x_i a_j^i y^j$$

is called a bilinear form in these two sets of variables. In matrix notation, it can be written as

$$q = \mathbf{x}A\mathbf{y}, \qquad \mathbf{x} = (x_i)_{1\times m}, \quad A = (a_j^i)_{m\times n}, \quad \mathbf{y} = (y^j)_{n\times 1}.$$

Show that there exist invertible changes of variables

$$x_i = \sum_{k=1}^{m} t_k p_i^k, \quad i = 1, \cdots, m, \qquad y^j = \sum_{l=1}^{n} q_l^j s^l \quad j = 1, \cdots, n,$$

i.e., $\mathbf{x} = \mathbf{t}P$ and $\mathbf{y} = Q\mathbf{s}$, where P and Q are invertible matrices, such that

$$q = \sum_{k=1}^{r} t_k s^k$$

where r is the rank of the matrix A.

Exercise 7. *Let $\mathbf{A} : U \to V$ be a linear map and A be the matrix of the map under bases $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ of U and $\{\mathbf{v}_1 \cdots, \mathbf{v}_m\}$ of V. Suppose $\mathbf{A}\mathbf{x} = \mathbf{y}$. Denote by $x = (x^1 \ \cdots \ x^n)^T \in \mathbb{F}^n$ and by $y = (y^1 \cdots \ y^m)^T \in \mathbb{F}^m$ the coordinates of $\mathbf{x}$ and $\mathbf{y}$ under the bases; i.e. $\mathbf{x} = \sum_{j=1}^{n} \mathbf{u}_j x^j$ and $\mathbf{y} = \sum_{i=1}^{m} \mathbf{v}_i y^i$. Show that*

$$y = Ax$$

Exercise 8. *Consider a linear transformation $\mathbf{A} : \mathbf{x} \in \mathbb{F}^n \to A\mathbf{x} \in \mathbb{F}^m$, where $A \in M_{m,n}(\mathbb{F})$. Show that there are basis $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ of $\mathbb{F}^n$ and basis $\{\mathbf{v}_1, \cdots, \mathbf{v}_m\}$ of $\mathbb{F}^m$ such that*

$$\mathbf{A}(\mathbf{u}_i) = \mathbf{v}_i \quad \forall i = 1, \cdots, r, \qquad A\mathbf{u}_i = \mathbf{0} \quad \forall i = r+1, \cdots, n$$

where r is the rank of the matrix A. That is, the matrix of the linear map $\mathbf{A}$ under the basis $\{\mathbf{u}_1, \cdots, \mathbf{u}_n\}$ and $\{\mathbf{v}_1, \cdots, \mathbf{v}_m\}$ is $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Consequently, the range of $\mathbf{A}$ is $\operatorname{span}\{\mathbf{v}_1, \cdots, \mathbf{v}_r\}$ and the null space (kernel) of $\mathbf{A}$ is $\operatorname{span}\{\mathbf{u}_{r+1}, \cdots, \mathbf{u}_n\}$.

Exercise 9. *Show that if A is reduced to an identity matrix by a succession of of column operations, the same succession of column operations performed on the identity matrix produces A^{-1}.*

Also prove Theorem 5.1 (4).

Exercise 10. *Consider the linear system $A\mathbf{x} = \mathbf{b}$ where $A \in M_{m,n}(\mathbb{F})$ and $\mathbf{b} \in \mathbb{F}^m$ are given and $\mathbf{x} \in \mathbb{F}^n$ is the unknown. Show that there are invertible matrices $P \in M_m(\mathbb{F})$ and $Q \in M_n(\mathbb{F})$ such that after the invertible change of variables $\mathbf{z} := (z^1 \ \cdots \ z^n)^T = Q\mathbf{x}$, the system is equivalent to*

$$\begin{aligned} z^i &= \bar{b}^i \quad \forall\, i = 1, \cdots, r, \\ 0 &= \bar{b}^j \quad \forall\, j = r+1, \cdots, m, \end{aligned}$$

where $\bar{\mathbf{b}} = (b^1 \ \cdots \ \bar{b}^m) := P\mathbf{b}$ and r is the rank of A.

Consequently, the following holds:

(i) If $r = m$ or $r < m$ and $0 = \bar{b}^j$ for all $j = r+1, \cdots, m$, then the system $A\mathbf{x} = \mathbf{b}$ is solvable, and all solutions are given by

$$\mathbf{x} = \sum_{i=1}^{r} \mathbf{q}_i b^i + \sum_{j=r+1}^{n} \mathbf{q}_j c^j$$

where $\mathbf{q}_1, \cdots \mathbf{q}_n$ are the column vectors of Q^{-1}, and $c^{r+1}, \cdots, c^n$ are arbitrary constants.

In particular, if $r = n$, then the solution is unique.

(ii) If $r < m$ and $\bar{b}^j \neq 0$ for some $j \in \{r+1, \cdots, m\}$, then the system $A\mathbf{x} = \mathbf{b}$ is not solvable.

Exercise 11. *Prove that the equivalence relation divides $M_{m,n}(\mathbb{F})$ into $1 + \min\{m, n\}$ equivalent classes.*

Exercise 12. *Let $\mathbf{x}_1 \cdots, \mathbf{x}_k$ be column vectors in $\mathbb{F}^m$ and $\mathbf{y}^1, \cdots, \mathbf{y}^k$ be row vectors in $\mathbb{F}_n$. Define*

$$A = \sum_{i=1}^{k} \mathbf{x}_i \mathbf{y}^i = (\mathbf{x}_1 \ \cdots \ \mathbf{x}_k) \begin{pmatrix} \mathbf{y}^1 \\ \vdots \\ \mathbf{y}_k \end{pmatrix} \in M_{m,n}(\mathbb{F}).$$

Prove the following:

(i)the row space of A is a subspace of $\operatorname{span}\{\mathbf{y}^1, \cdots, \cdots \mathbf{y}^k\}$; in addition, if $\{\mathbf{x}_1, \cdots, \mathbf{x}_k\}$ is linearly independent, then the row space of A is equal to $\operatorname{span}\{\mathbf{y}^1, \cdots, \mathbf{y}^k\}$.

(ii) the column space of A is a subspace of $\operatorname{span}\{\mathbf{x}_1, \cdots, \mathbf{x}_k\}$; in addition, if $\{\mathbf{y}^1, \cdots, \mathbf{y}^k\}$ is linearly independent, then the column space of A is equal to $\operatorname{span}\{\mathbf{x}_1, \cdots, \mathbf{x}_k\}$.

Exercise 13. * *Find invertible matrices $P \in M_2(\mathbb{Z})$ and $Q \in M_3(\mathbb{Z})$ such that $PAQ = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \end{pmatrix}$ and d_1 divides d_2, for*

$$A = \begin{pmatrix} 3 & 8 & 10 \\ 4 & 9 & 20 \end{pmatrix}, \qquad A = \begin{pmatrix} 14 & 18 & 12 \\ 22 & 6 & 30 \end{pmatrix}.$$

5.3 Congruence

A **quadratic form** of n variables $x^1, \cdots, x^n$ is a degree 2 polynomial

$$q = \sum_{i,j=1}^{n} x^i a_{ij} x^j = \mathbf{x}^T A \mathbf{x} = \tfrac{1}{2}\mathbf{x}^T (A^T + A)\mathbf{x}, \qquad \mathbf{x} = (x^i)_{n\times 1}, \quad A = (a_{ij})_{n\times n}.$$

Under a linear invertible change of variables

$$x^i = \sum_{k=1}^{n} p^i_k y^k, \quad i = 1, \cdots, n, \qquad \text{i.e.} \quad \mathbf{x} = P\mathbf{y}$$

the quadratic form becomes

$$q = \mathbf{x}^T A \mathbf{x} = \mathbf{y}^T B \mathbf{y}, \qquad B = P^T A P.$$

Definition 5.5. *Two matrices A and B are called* **congruent** *if $B = P^T AP$ for some invertible P.*

Notice that for two matrices to be congruent, they have to be square and of same dimension.

Congruence is an RST relation on square matrices. In addition, congruence is a sub-relation of the equivalence relation, so the ranks of congruent matrices are equal.

Since the congruence relation originates from quadratic forms, most of the known results about congruence are confined to symmetric matrices.

Theorem 5.2. *1. Two matrices are congruent if and only if one is obtained from the other by a succession of pair of elementary operations, each pair consisting of a column operation and the corresponding row operation. In each pair either operation can be performed first.*

The succession of elementary operations can be recorded as, for $P = E_1 \cdots E_k$,

$$\begin{pmatrix} A \\ I \end{pmatrix} \longrightarrow \begin{pmatrix} E_k^T \cdots E_1^T A E_1 \cdots E_k \\ I E_1 \cdots E_k \end{pmatrix} \qquad \begin{matrix} E_k^T \cdots E_1^T I \end{matrix} = \begin{pmatrix} P^T A P & P^T \\ P \end{pmatrix}.$$

2. Over any field in which $1 + 1 \neq 0$, each symmetric matrix is congruent to a diagonal matrix in which the number of non-zero diagonal entries is the rank of A.

3. A complex symmetric matrix of rank r is congruent to a matrix $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

4. A real symmetric matrix is congruent over $\mathbb{R}$ to a matrix

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where (p, q), called the **index pair** *of A, is uniquely determined by A.*

Proof. 1. Each invertible matrix P is a product of elementary matrices: $P = E_1 E_2 \cdots E_k$. Thus, $B = P^T AP$ if and only if

$$B = E_k^T [\cdots (E_1^T A E_1) \cdots] E_k.$$

For each elementary column operation effected by E_i as a right factor the corresponding row operation is effected by E_i^T as a left factor. Hence, $B = P^T BP$ if and only if B is obtained from A by performing a succession of pairs of elementary operations. The final statement of the first assertion of the theorem merely amounts to the associative law $E_i^T (C E_i) = (E_i^T C) E_i$.

Note that $P = IE_1 \cdots E_k$ is obtained by applying successively the corresponding column operations on I, and $P^T = E_k \cdots E_1^T I$ is obtained by applying successively the corresponding row operations on I.

2. If $A = 0I$, then the desired matrix is A itself. Hence we assume that $A = A^T \neq 0I$.

Next we show that A is congruent to a matrix B with a non-zero diagonal entry. This is true if A has a non-zero diagonal element, since we can take $B = A = I^T AI$. Hence, we assume that $a_{jj} = 0$ for all j. Since $A \neq 0I$, there is $a_{ij} = a_{ji} \neq 0$ for some $i \neq j$. Addition of column j to column i followed by addition of row j to row i replace A by a congruent matrix $B = (b_{kl})_{n\times n}$ in which $b_{ii} = a_{ii} + a_{jj} + a_{ji} + a_{ij} = 2a_{ij} \neq 0$.

An interchange of column 1 and column i in B followed by the corresponding row operation replace B by $C = (c_{kl})_{n\times n}$ with $c_{11} = b_{ii} \neq 0$.

Now we add to column j the product of the first column by $-c_{1j}/c_{11}$, then perform the corresponding row operation. Since $c_{1j} = c_{j1}$, this makes the new elements in the $(1, j)$ and $(j, 1)$ places both 0. Doing this for $j = 2, \cdots, n$, we replace C by a matrix $\begin{pmatrix} c_{11} & 0 \\ 0 & A_1 \end{pmatrix}$ where A_1 is a symmetric $(n-1) \times (n-1)$ matrix. (Is computation necessary to verify the symmetry of A_1?)

The same procedure may be applied to A_1 with operations not affecting the first row or column. After finite number of steps, there appears a diagonal matrix congruent to A. Preservation of rank is a consequence of the fact that congruence is a special case of equivalence.

3. The third assertion follows from the second assertion, since every complex number has a square root.

4. From 2, $A = P^T DP$ where $D = \text{diag}(d_1, \cdots, d_r, 0, \cdots, 0)$ where each d_i is non-zero. Let p be the number of d_h which are positive. By suitable interchange of rows followed by the corresponding column interchanges, these p elements may be brought into the first p position. Let $c_i = \sqrt{|d_i|}$ for $i = 1, \cdots, r$. For each $i = 1, \cdots, r$, multiplication the ith column by $1/c_i$ followed by the corresponding row operation, D then is then congruent to the matrix in the theorem.

It remains to show that (p, q) is unique. Suppose A is also congruent to another diagonal matrix with index (p', q'). If $p \neq p'$, it is a matter of notation to assume that $p' < p$.

Consider the quadratic form $f = \mathbf{x}^T A\mathbf{x}$. Under invertible linear substitution $\mathbf{x} = P\mathbf{y}, \quad \mathbf{x} = Q\mathbf{z}$, we obtain

$$f = (y^1)^2 + \cdots + (y^p)^2 - (y^{p+1})^2 - \cdots - (y^r)^2 = (z^1)^2 + \cdots + (z^{p'})^2 - (z^{p'+1})^2 - \cdots - (z^r)^2$$

where $r = p + q = p' + q'$ is the rank of A. As $\mathbf{y} = P^{-1}\mathbf{x}$ and $\mathbf{z} = Q^{-1}\mathbf{x}$, the system of equations

$$z^i = 0, \quad y^j = 0, \qquad h = 1, \cdots, p', j = p + 1, \cdots, n$$

can be regarded as simultaneous linear, homogeneous equations in $x^1, \cdots, x^n$. There are n unknowns and $p' + (n - p) < n$ equations, hence there exists a non-trivial solution $\mathbf{x}_0$. Set $\mathbf{y}_0 = P\mathbf{x}_0 = (y_0^k)$ and $\mathbf{z}_0 = Q\mathbf{x}_0 = (z_0^k)$. Then the value of f at $\mathbf{x}_0$ can write as

$$f = \mathbf{x}_0^T A\mathbf{x}_0 = \sum_{k=1}^{p} (y_0^k)^2 = -\sum_{k=p'+1}^{r} (z_0^k)^2$$

from which we conclude that $y_0^i = 0$ for all $i = 1, \cdots, p$, which implies that $\mathbf{y}_0 = \mathbf{0}$, and consequently, $\mathbf{x}_0 = P^{-1}\mathbf{y}_0 = \mathbf{0}$, a contradiction. Thus $p = p'$. □

A matrix A is called **skew** or **skew-symmetric** if $A = -A^T$. There are many reasons for interest in skew matrices. One is that any square matrices A can be written uniquely as $A = S + K$ where S is symmetric and K is skew. Indeed, $S = \frac{1}{2}(A + A^T)$ and $K = \frac{1}{2}(A - A^T)$.

Although there is no good result on congruence for general square matrices, it is interesting and surprising to find that we can with very little effort to get a canonical set for skew symmetric matrices.

We first note that a matrix congruent to a skew matrix is also skew:

$$(P^TAP)^T = P^TA^TP = -P^TAP \quad \text{if} \quad A^T = -A.$$

Also we notice that if $2 \neq 0$, then all diagonal entries of a skew matrix is zero.

Theorem 5.3. *Assume that $\mathbb{F}$ is a field in which $1+1 \neq 0$.*

1. *Each skew matrix over $\mathbb{F}$ is congruent over $\mathbb{F}$ to a matrix $B = \operatorname{diag}(E, \cdots, E, 0)$ where 0 is a zero matrix of suitable size (possibly absent) and $E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.*
2. *Two $n \times n$ skew matrix over $\mathbb{F}$ is congruent over $\mathbb{F}$ if and only if they have the same rank.*

Proof. If $A = 0I$, we take $B = A$. Otherwise, there is $a_{ij} = -a_{ji} = c \neq 0$ where $i \neq j$. Multiplication of row j and column j by $1/c$ we can assume that $a_{ij} = 1$.

Interchange of row i with row 1, of column i with column 1, of row j with row 2, of column j with column 2, A is then congruent to a skew matrix $C = \begin{pmatrix} E & C_1 \\ -C_1^T & C_2 \end{pmatrix}$.

It is clear that the element -1 in E may be exploited by row operations to make the first column of $-C_1$ zero; the corresponding column operations makes the first row of C_1 zero. Likewise, the second column of $-C_1$ can be made zero by use of the $+1$ in E, and the second row of C_1 can be made zero. Thus, A is congruent to $\begin{pmatrix} E & 0 \\ 0 & A_1 \end{pmatrix}$.

An induction then completes the proof. □

Example 5.2. *Find an invertible matrix P such that P^TAP is triangular and equivalent to $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.*

Solution. For the matrix $\begin{pmatrix} A \\ I \end{pmatrix}$ we perform successively row operations and corresponding column operations on the first n rows and columns. The following records the change of the first n rows: $(A\ I) =$

$$\begin{pmatrix} 0 & 2 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} 3 & 2 & 1 & 1 \\ 0 & -2/3 & -1/3 & 2/3 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 1 & 1 & 1 \\ 0 & -2/3 & -1/3 & 2/3 \end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} \sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ 0 & -2/3 & -1/3 & 2/3 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ 0 & -2/3 & -1/3 & 2/3 \end{pmatrix}$$

Hence, set $P^T = \begin{pmatrix} 1/\sqrt{3} & 1/\sqrt{3} \\ -1/3 & 2/3 \end{pmatrix}$, i.e. $P = \begin{pmatrix} 1/\sqrt{3} & -1/3 \\ 1/\sqrt{3} & 2/3 \end{pmatrix}$ we have $P^TAP = \begin{pmatrix} 1 & 1/\sqrt{3} \\ 0 & -2/3 \end{pmatrix}$.

Exercise 14. *For $E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, show that $E^2 = -I$.*

Exercise 15. *Use the scheme in the proof transform congruently the following matrices into triangular forms:*

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 2 \\ 10 & 0 & 3 \\ 2 & 3 & 0 \end{pmatrix}$$

Exercise 16. *For the following quadratic forms, find a change of variable* $\mathbf{y} = P\mathbf{x}$ *such that they become diagonal forms.*

(a) $f = xy + yz$, *where* $(x, y, z)^T \in \mathbb{R}^3$;
(b) $f = x^2 - y^2 + 2\mathbf{i}xy$, *where* $(x, y)^T \in \mathbb{C}^2$;
(b) $g = ax^2 + 2bxy + cy^2$, *where* $(x, y) \in \mathbb{R}^2$, $a, b, c \in \mathbb{R}$,
(c) $h = \left(\sum_{i=1}^n a_i x^i\right)\left(\sum_{j=1}^n b_j x^j\right)$ *where* $(x^i) \in \mathbb{R}^n$.

Exercise 17. *Prove that if* A *is skew, then* A^2 *is symmetric.*

Exercise 18. *Find a invertible matrix* P *such that* $P^T AP$ *is in the canonical form, where* A *is one of the following*

$$\begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 3 \\ -2 & -3 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & 1 & 0 \\ -1 & -1 & 0 & -2 \\ -1 & 0 & 2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \mathbf{i} \\ -\mathbf{i} & 0 \end{pmatrix}$$

Exercise 19. *Show that congruence (over* $\mathbb{R}$*) relation divides all* $n \times n$ *real symmetric matrices into* $\frac{1}{2}(n+1)(n+2)$ *equivalent classes.*

5.4 Hermitian Congruence

In defining inner product on $\mathbb{C}^n$, we need to work on **Hermitian forms**,

$$q = \sum_{i=1}^{n}\sum_{j=1}^{n} \bar{z}^i a_{ij} z^j = \mathbf{z}^* A\mathbf{z} \qquad \mathbf{z} = (z^i) \in \mathbb{C}^n, \mathbf{z}^* := \bar{\mathbf{z}}^T, \quad A = (a_{ij}) \in M_n(\mathbb{C}).$$

Note that a change of variable $\mathbf{w} = P\mathbf{x}$ gives

$$q = \mathbf{z}^* A\mathbf{z} = \mathbf{y}^* B\mathbf{y}, \quad B = P^* AP.$$

Definition 5.6. *Two square matrices A and B in $M_n(\mathbb{C})$ are called* **Hermitely congruent** *if $B = P^*AP$ for some invertible $P \in M_n(\mathbb{C})$, where $P^* := \bar{P}^T$.*

A matrix $A \in M_n(\mathbb{C})$ is called **Hermitain** *if $A^* = A$.*

A matrix $A \in M_n(\mathbb{C})$ is called **Skew-Hermitian** *if $A^* = -A$, i.e., $\mathbf{iA}$ is Hermitian.*

A matrix $A \in M_m(\mathbb{C})$ is called **positive definite** *if $\mathbf{z}^*A\mathbf{z} > 0$ for all non-trivial $\mathbf{z} \in \mathbb{C}^n$.*

A matrix $A \in M_m(\mathbb{R})$ is called **positive definite** *if $A = A^T$ and $\mathbf{x}^T A\mathbf{x} > 0$ for all non-trivial $\mathbf{x} \in \mathbb{R}^n$.*

Note that the value of a Hermitian form $q = \mathbf{z}^*A\mathbf{z}$ is real for all $\mathbf{z} \in \mathbb{C}^n$ if and only if A is **Hermitian**. Hence, the two definitions of positive definite are consistent.

Also note that a matrix that is Hemitely congruent to a Hermitian matrix is also Hermitian.

The reduction theory for Hermitian matrices under Hermitely congruence is an almost perfect analogues of the theory for symmetric matrices relative to congruence, and the proof requires only minor changes.

Theorem 5.4. *1. Two matrices in $M_n(\mathbb{C})$ are Hemitely congruent if and only if one is obtained from the other by a succession of pairs of elementary operations, each pair consisting of an elementary column operation and the conjunctively corresponding row operation; namely, A and B are Hermitely congruent if and only if*

$$B = E_k^*[\cdots(E_1^* A E_1)\cdots]E_k$$

where $E_1, \cdots, E_k$ are elementary matrices. In particular, $B = P^*AP$ where $P^* = E_k^* \cdots E_1^* I$ is obtained by performing successively row operations $\mathcal{O}_1^*, \cdots, \mathcal{O}_k^*$ on I, and $P = IE_1 \cdots E_k$ is obtained by performing successively column operations $\mathcal{O}_1, \cdots, \mathcal{O}_k$ on I.

2. Every Hermitian matrix is Hermitely congruent to a matrix of the form

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where the integer **index pair** *(p, q) is uniquely determined by A.*

3. A matrix A is positive definite if and only if it is Hermitely congruent to an identity matrix; namely, $A = P^*P$ where P is an invertible matrix.

4. Every skew-Hermitian matrix is Hermitely congruent to a matrix of the form

$$\begin{pmatrix} \mathbf{i}I_p & 0 & 0 \\ 0 & -\mathbf{i}I_q & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where the integer **index pair** *(p, q) is uniquely determined by A.*

Exercise 20. *Prove Theorem 5.4.*

Exercise 21. *Let $A \in M_n(\mathbb{C})$. In $\mathbb{C}^n$, define a sesqui-bilinear form*

$$\langle \mathbf{x}, \mathbf{y} \rangle := \mathbf{y}^* A \mathbf{x} \qquad \forall\, \mathbf{x}, \mathbf{y} \in \mathbb{C}^n.$$

(i) Show that $\langle \cdot, \cdot \rangle$ is an inner product if and only if A is positive definite.

(ii) Suppose $A = P^*P$ where $P \in M_n(\mathbb{C})$ is invertible. Write $P^{-1} = (\mathbf{v}_1 \cdots \mathbf{v}_n)$. Show that $\{\mathbf{v}_1, \cdots, \mathbf{v}_n\}$ is an orthonormal basis under the inner product $\langle \cdot, \cdot \rangle$.

Exercise 22. *Suppose $A = B + \mathbf{i}C$ where $A \in M_n(\mathbb{C})$ is Hermitian, and $B, C \in M_n(\mathbb{R})$. Show that B is symmetric and C is skew-symmetric.*

Exercise 23. *Let $A \in M_n(\mathbb{C})$. Show that A can be written uniquely as $A = B + \mathbf{i}C$ where both B and C are Hermitian.*

Exercise 24. *Find invertible $P \in M_n(\mathbb{C})$ such that P^*AP is in its canonical form, for the following A's:*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}, \qquad \begin{pmatrix} 2 & \mathbf{i} \\ -\mathbf{i} & 2 \end{pmatrix}$$

Exercise 25. *Define an inner product on $\mathbb{C}$ by $\langle \mathbf{x}, \mathbf{y} \rangle := \mathbf{y}^* A \mathbf{x}$ where A is as the last matrix in the previous exercise. Find an orthonormal basis.*

Exercise 26. *Let $A \in M_n(\mathbb{C})$. (i) Show that if $\mathbf{x}^* A \mathbf{x} = 0$ for all $\mathbf{x} \in \mathbb{C}$, then $A = 0I$.*

(ii) Sow that A is Hermitian if and only if $\mathbf{x}^* A \mathbf{x} \in \mathbb{R}$ for all $\mathbf{x} \in \mathbb{C}^n$.

Exercise 27. * *Let A be a Hermitian matrix.*

(i) Show that any principal sub-matrix of A (a square matrix obtained from A by deleting some rows and corresponding columns) is also Hermitian.

(ii) Using an induction argument on the dimension of A show that A is positive definite if and only if $\det(S_j) > 0$ for all $j = 1, \cdots, n$ where S_j is the submatrix of A taken from the first j rows and columns.

Hint: Suppose $P^*AP = I$. Then

$$\begin{pmatrix} P^* & \mathbf{0} \\ \mathbf{0}^* & 1 \end{pmatrix} \begin{pmatrix} A & B \\ B^* & c \end{pmatrix} \begin{pmatrix} P & \mathbf{0} \\ \mathbf{0}^* & 1 \end{pmatrix} = \begin{pmatrix} I & P^*B \\ B^*P & c \end{pmatrix}$$

$$\begin{pmatrix} I & \mathbf{0} \\ -B^*P & 1 \end{pmatrix} \begin{pmatrix} I & P^*B \\ B^*P & c \end{pmatrix} \begin{pmatrix} I & -P^*B \\ \mathbf{0}^* & 1 \end{pmatrix} = \begin{pmatrix} I & \mathbf{0} \\ \mathbf{0}^* & d \end{pmatrix}$$

where $d = \left|\det(P)\right|^2 \det \begin{pmatrix} A & B \\ B^* & c \end{pmatrix}$.

5.5 Polynomials over a Field

Let $\mathbb{F}$ be a field and x be an abstract symbol. A **polynomial** in the symbol x with coefficient in $\mathbb{F}$ is an expression

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + cx + c_0 x^0.$$

where n is a non-negative integer and each c_i is in $\mathbb{F}$. If all c_i are zero, we call it the zero polynomial, and is denoted by $\mathbf{0}$. If $c_n \neq 0$, then c_n is called the **leading coefficient** of $p(x)$ and n is called the **degree** of p and write

$$n = \deg(p(x)).$$

If its lading coefficient is 1, $p(x)$ is called **monic**. The degree of a non-zero constant (times x^0) is zero, and the degree of a zero polynomial is defined as $-\infty$.

The set of all polynomials in x with coefficients in $\mathbb{F}$ is denoted by $\mathbb{F}[x]$ (read " $\mathbb{F}$ bracket x"). If we abandon the notion of x as variable, we may regard each $p(x)$ as a single, fixed entity, a member of the set $\mathbb{F}[x]$. We equip $\mathbb{F}[x]$ with the conventional summation and multiplications,

$$1 \cdot x = x, \quad 0 \cdot x = \mathbf{0}, \quad cx = xc, \quad x^i \cdot x^j = x^{i+j},$$
$$\textstyle\sum_i c_i x^i + \sum_j d_j x^j = \sum_k (c_k + d_k) x^k,$$
$$\textstyle\sum c_i x^i \sum d_j x^j = \sum_{i,j} c_i d_j x^{i+j}.$$

Then $\mathbb{F}[x]$ becomes a commutative ring, which we call it a **polynomial domain** over $\mathbb{F}$.

Remark: (i) If x is a variable taking values in $\mathbb{F}$, then $x^0 = 1 \in \mathbb{F}$ and $\mathbf{0} = 0$.

(ii) If x is a variable taking values in $M_n(\mathbb{F})$, than $x^0 = I$ and $\mathbf{0} = 0I$.

(iii) In default, x is an abstract symbol, and therefore so are x^n. For simplicity, we abuse 0 for $\mathbf{0}$ and c for cx^0.

Example 5.3. Let $\mathbb{F} = \{0, 1\}$ equipped with the mod (2) integer arithmetic. Consider the polynomial

$$f(x) = x^2 - x = x(x-1).$$

If we regard x as a variable in $\mathbb{F}$, then $f(x) \equiv 0$. However, we regard x as an abstract symbol, so that $f(x) \neq 0$ and $\deg(f) = 2$.

Since x is regarded as a symbol, for any field $\mathbb{F}$, we have the following: For any non-zero polynomial $p(x)$ and $q(x)$,

$$\deg(pq) = \deg p + \deg(q)$$

This property implies that if $f(x)g(x) = 0$ then either $f(x) = 0$ or $g(x) = 0$. Note that the definition that the degree of zero polynomial is $-\infty$ is consistent with the above degree formula. Also, we have a cancellation law:

If $h(x)g(x) = f(x)g(x), \quad g(x) \neq 0$, then $h(x) = f(x)$.

Given polynomials $f(x)$ and $g(x)$ over $\mathbb{F}$, we say $g(x)$ divides $f(x)$, or $g(x)$ is a **factor** of $f(x)$ if $f(x) = g(x)h(x)$ for some $h(x) \in \mathbb{F}[x]$. In such a case, we write $g|f$. Note that $g|0$ for any g.

An expression $f(x) = g(x)h(x)$ is called a **factorization** of $f(x)$. A factorization of two factors, of which one is a constant, will be called a trivial factorization.

Definition 5.7. *1. A non-constant polynomial is called* **irreducible** *over $\mathbb{F}$ is all of its factorizations into two factors over $\mathbb{F}$ are trivial.*

2. *If a polynomial $g(x)$ divides both $f_1(x)$ and $f_2(x)$, $g(x)$ is called a* **common divisor** *of $f_1(x)$ and $f_2(x)$.*

3. *A monic polynomial is called the* **greatest common divisor**, *or simply* **gcd**, *of $f_1(x)$ and $f_2(x)$ if (a) $g(x)$ is a common divisor of $f_1(x)$ and $f_2(x)$ and (b) every common divisor of $f_1(x)$ and $f_2(x)$ is a divisor of $g(x)$.*

4. *Two polynomials are called* **relatively prime** *if their gcd is unit.*

Note that every degree 1 polynomial is irreducible. In $\mathbb{Q}[x]$, $x^2 - 2$ is irreducible. In $\mathbb{R}[x]$, $x^4 + 1$ is also irreducible. Also, we take the default that the gcd of a non-zero polynomial f and the zero polynomial is cf, where c is a scalar so that cf is monic. Also, the gcd of two zero polynomials is zero.

The familiar process of long division of polynomials is valid over an arbitrary field. The following lemma, known as **divisor algorithm**, is a careful formulation of the result of dividing as far as possible.

Lemma 5.4. *If $f(x)$ and $g(x)$ are polynomials over $\mathbb{F}$ and $g(x) \neq 0$, then there are unique polynomials $q(x)$ and $r(x)$ over $\mathbb{F}$ such that*

$$f(x) = q(x)g(x) + r(x), \qquad \text{either } \ r(x) = 0 \ \text{ or } \ \deg(r(x)) < \deg(g(x)).$$

One notices that if $f(x)$ divides by $x - c$ (indeed $x - cx^0$), the remainder is $f(c)$ (indeed, $f(c)x^0$). Consequently, $x - c$ divides $f(x)$ if and only if $f(c) = 0$, i.e. c is a root of $f(x) = 0$.

Theorem 5.5. *If both $f_1(x)$ and $f_2(x)$ are non-zero polynomials over $\mathbb{F}$, they have a greatest common divisor $d(x)$ in $\mathbb{F}[x]$. Moreover, $d(x)$ is unique and is expressible as*

$$d(x) = p_1(x)f_1(x) + p_2(x)f_2(x)$$

where $p_1(x), p_2(x) \in \mathbb{F}[x]$.

In particular, $f(x)$ and $g(x)$ is prime to each other if and only there are $a(x)$ and $b(x)$ in $F[x]$ such that

$$1 = a(x)f(x) + b(x)g(x).$$

We shall use the notation

$$d(x) = \gcd[f_1(x), f_2(x)]$$

for the greatest common divisor of $f_1(x)$ and $f_2(x)$. The gcd can be found by the following algorithm:

$$\begin{aligned}
f_1 &= q_1 f_2 + f_3, && \deg(f_3) < \deg(f_2),\\
f_2 &= q_2 f_3 + f_4, && \deg(f_4) < \deg(f_3),\\
&\cdots\cdots && \\
f_k &= q_k f_{k+1} + f_{k+2}, && \deg(f_{k+2}) < \deg(f_{k+1}),\\
f_{k+1} &= q_{k+1} f_{k+2}. &&
\end{aligned}$$

Then $d(x) = cf_{k+2}(x)$ where c is a constant. One can use these equations to express f_{k+2} as a linear combination of f_1 and f_2.

Theorem 5.6. *Every non-zero polynomial $f(x)$ over $\mathbb{F}$ is expressible in the form*

$$f(x) = cp_1(x) \cdots p_r(x)$$

where c is a non-zero constant and each $p_i(x)$ is a monic, irreducible polynomial of $\mathbb{F}[x]$. The above factorization is unique apart from the order in which the factors of $p_i(x)$ appear.

The above theorem is usually called the **unique factorization theorem**.

Although irreducibility of a polynomial depend on the size of a field, the concept of greatest common divisor and therefore also relative prime are independent of the field used.

Theorem 5.7. *Let $\mathbb{F}$ and $\mathbb{K}$ be two fields sauch that $\mathbb{F} \subset \mathbb{K}$. Suppose $f(x), g(x) \in \mathbb{F}[x]$. Then the their* gcd *within $\mathbb{F}[x]$ is also their* gcd *in $\mathbb{K}[x]$.*

In particular, if $f(x)$ and $g(x)$ are prime to each othr in $\mathbb{F}[x]$, then they are also prime to each other in $\mathbb{K}[x]$.

Proof. Let $d(x)$ be the gcd of f and g in $\mathbb{K}[x]$ and $D(x)$ be their gcd in $\mathbb{K}[x]$. Since $\mathbb{F} \subset \mathbb{K}$, $d(x)|D(x)$.

Let $a(x)$ and $b(x)$ in $\mathbb{F}[x]$ be such that

$$d(x) = a(x)f(x) + b(x)g(x).$$

Also let $p(x), q(x) \in \mathbb{K}[x]$ be such that $f(x) = p(x)D(x)$ and $g(x) = q(x)D(x)$. Then

$$d(x) = a(x)p(x)D(x) + b(x)q(x)D(x) = h(x)D(x)$$

where $h(x) \in \mathbb{K}[x]$. Since $d(x)|D(x)$, we must have $\deg(h) = 1$, namely, h is a constant in $\mathbb{K}$. As both $D(x)$ and $d(x)$ are monic polynomials, we must have $h(x) = 1$. Hence, $d(x) = D(x)$. □

Exercise 28. *Define the greatest common divisor for multiple non-trivial polynomials $f_1(x), \cdots, f_k(x)$. Show that $d(x) = \gcd[f_1(x), \cdots, f_k(x)]$ exists, and there exists $a_1(x), \cdots, a_k(x)$ such that*

$$d(x) = a_1(x)f_1(x) + \cdots + a_k(x)f_k(x).$$

Exercise 29. *(1) Suppose $p(x)$ is prime to each of $f_1(x), \cdots, f_k(x)$. Show that $p(x)$ is prime to $\Pi_{i=1}^k f_i(x)$.*

(2) Suppose p is irreducible and $p|f_1 \cdots f_k$. Show that $p|f_i$ for some $i \in \{1, \cdots, k\}$.

Exercise 30. *Let $R = \{m + n\sqrt{5}\mathbf{i} \mid m, n \in \mathbb{Z}\}$, equipped with the arithmetic of complex numbers. Show that R is a ring, i.e. R is closed under summation, negation, and multiplication. Also show that $1+\sqrt{5}\mathbf{i}$, $1-\sqrt{5}\mathbf{i}$, $2, 3$ are all prime numbers. Nevertheless, $6 = 2 * 3 = (1+\sqrt{5}\mathbf{i})(1-\sqrt{5}\mathbf{i})$, so that R is not a unique factorization ring.*

Exercise 31. *Find a, b such that $\gcd[f_1, f_2] = af_1 + bf_2$ where $f_1 = x^4 - 3x^2 + 3$ and $f_2 = x^3 + x^2 + x + 1$.*

Exercise 32. *Suppose both f and g are non-zero polynomials. Show that there exist a, b such that $\deg(b) < \deg(f)$, $\deg(a) < \deg(g)$ and $\gcd[f, g] = af + bg$.*

5.6 Equivalence over $\mathbb{F}[x]$

Many of the fundamental and practical results in the theory of matrices occur in the study of similar matrices, and in related subjects. Though matrices in question may have real number entries, the proofs of theorems, and sometimes the theorem too, involve certain other matrices whose entries are polynomials. It is largely for this reason that we study matrices with polynomial entries. The main theme in this section is the theory of equivalence relations over $\mathbb{F}[x]$.

In this section, we consider matrices $A = A(x)$ in $M_{m,n}(\mathbb{F}[x])$, i.e., rectangular matrices with entries in $\mathbb{F}[x]$.

Definition 5.8. *1. Elementary operation on a matrix over $\mathbb{F}[x]$ are defined as follows:*

(a) Interchange of two rows (or two columns).

(b) Multiplication of a row (or column) by a non-zero constant (scalar).

(c) Addition to one row (or column) by a polynomial multiple of another row (or column).

Elementary matrices over $\mathbb{F}[x]$ are those that obtained from I after a single elementary operation on matrix over $\mathbb{F}[x]$.

2. *A square matrix A over $\mathbb{F}[x]$ is called invertible over $\mathbb{F}[x]$ if there is a matrix B over $\mathbb{F}[x]$ such that $AB = BA = I$.*

3. *Two matrices A and B over $\mathbb{F}[x]$ are called* **equivalent over** *$\mathbb{F}[x]$ if $B = PAQ$ where P and Q are matrices over $\mathbb{F}[x]$ that are invertible over $\mathbb{F}[x]$.*

First we study invertible matrices; namely, those matrices that are equivalent over $\mathbb{F}[x]$ to the identity matrix.

Lemma 5.5. *1. Every elementary matrix over $\mathbb{F}[x]$ has an inverse which is also elementary.*

2. *A matrix over $\mathbb{F}[x]$ has an inverse if and only if its determinant is a non-zero constant.*

3. *Any matrix over $\mathbb{F}[x]$ that is invertible over $\mathbb{F}[x]$ if and only if it is the product of elementary matrices.*

4. *If a succession of elementary row operations over $\mathbb{F}[x]$ reduced a matrix into an identity matrix, then the same succession of operation on the identity matrix produces the inverse of the matrix.*

5. *Two matrices over $\mathbb{F}[x]$ are equivalent over $\mathbb{F}[x]$ if and only if one can be obtained from the other by a succession of elementary operations.*

Note that $\det(A) \neq 0$ for square matrix over $\mathbb{F}[x]$ does not imply that A is invertible; for example, for $A = x\mathbf{I} \in M_n(\mathbb{F}[x])$, $D(A) = x^n \neq 0$, but A is not invertible in $M_n(\mathbb{F}[x])$.

Next, we introduce **sub-matrix** and **sub-determinant**.

Definition 5.9. *Let A be a $m \times n$ matrix. A* **sub-matrix** *of A is a matrix obtained from A by deleting some rows and columns. A* **principal sub-matrix** *is a sub-matrix whose diagonal entries are also diagonal entries of A.*

A $t \times t$ **sub-determinant** *of A is the determinant of a $t \times t$ sub-matrix of A. A $t \times t$* **principal sub-determinant** *is the determinant of a $t \times t$ principal sub-matrix.*

Lemma 5.6. *Let $A, B \in M_{m,n}(\mathbb{F}[x])$ be two matrices equivalent over $\mathbb{F}[x]$. Then*

(1) Every $r \times r$ sub-determinant of A is a linear combination, with coefficients in $\mathbb{F}[x]$, of all $r \times r$ sub-determinants of B;

(2) the gcd *of all sub-determinants of A equals the* gcd *of all sub-determinants of B.*

Proof. (1) Suppose $A = EB$ where E is an elementary matrix over $\mathbb{F}[x]$, then E has three types. Performing the calculation for each of the three types, one can conclude that each $r \times r$ sub-determinant of A is a linear combination, with coefficients in $\mathbb{F}[x]$, of all $r \times r$ sub-determinants of B.

Similarly, the above assertion holds when $A = BE$ and E is an elementary matrix.

As every invertible matrix can be written as a product of elementary matrices, the first assertion thus follows.

(2) Let $d(x)$ and $D(x)$ be, respectively, the gcd of all $r \times r$ sub-determinants of A and B. Then $d(x)$ is a linear combination of all $r \times r$ sub-determinants of A, and by (1), is also a linear combination of all $r \times r$ sub-determinants of B, and hence, $D|d$ since D divides every $r \times r$ sub-determinants of B. As B is also equivalent to A, we also have $D|d$. Hence, $d = D$. □

Theorem 5.8. *Each matrix A over $\mathbb{F}[x]$ is equivalent over $\mathbb{F}[x]$ to a matrix*

$$S = \operatorname{diag}(f_1(x), \cdots, f_r(x), \mathbf{0})$$

where $f_1(x), \cdots, f_r(x)$ are monic polynomials satisfying $f_1(x)|f_2(x)|\cdots|f_r(x)$, and $\mathbf{0}$ is a $m-r$ by $n-r$ zero matrix.

In addition, such $S = S(x)$, called the **Smith's canonical matrix** *of $A = A(x)$, is unique, and for all $t = 1, \cdots, r$,*

$$g_t(x) := \Pi_{j=1}^{t} f_j(x)$$

is the gcd *of all $t \times t$ sub-determinants of A; in particular, denoting $g_0 = 1$,*

$$f_t(x) = \frac{g_t(x)}{g_{t-1}(x)} \quad \forall t = 1, \cdots, r.$$

The polynomials $f_1(x), \cdots, f_r(x)$ are called the **invariant factors** *of A.*

Two matrices in $M_{m,n}(\mathbb{F}[x])$ are equivalent over $\mathbb{F}[x]$ if and only if they have the same invariant factors, and also if and only if for all integer t satisfying $1 \le t \le \min\{m, n\}$, the gcd *of all $t \times t$ sub-determinants of one matrix equals that of the other matrix.*

Proof. Let $A \in M_{m,n}(\mathbb{F}[x])$ be given. Assume that $A \neq 0I$.

1. Let $k_1 \ge 0$ be the minimum degree of all non-zero elements of all matrices equivalent to A. Then there exists a monic polynomial $f_1(x)$ of degree k_1 such that $f_1(x)$ is an entry of a matrix $B = (b_{ij}(x))_{m\times n}$ equivalent to A. By interchange rows and columns, we can assume that $f_1(x) = b_{11}(x)$.

We claim that $f_1|b_{1j}$ for all $j = 2\cdots, n$. Suppose this is not true. Then for some $j \ge 2$, f does not divide b_{1j}. Hence, by a long division, we can write $b_{1j}(x) = a(x)f(x) + r(x)$ where $\deg(r) < \deg(f)$. Subtracting the first column multiplied by $a(x)$ from the jth column gives a new matrix equivalent to A and whose $(1, j)$ entry is $r(x)$. This contradicts the definition of k_1. Hence, $f_1|b_{1j}$. Similarly, we can show that $f_1|b_{j1}$ for all $j = 2, \cdots, m$.

Upon subtracting appropriate multiple of the first row/column from the jth row/column, we then obtain a matrix which is equivalent to A and has the form

$$B = \begin{pmatrix} f_1(x) & 0 \\ 0 & C \end{pmatrix}.$$

We claim that f_1 divides every entry of C. Suppose not. Then there is a non-zero entry $c_{ij}(x)$ of C such that f_1 does not divides c_{ij}. Adding the $(i+1)$th row of B to the first row, we obtain a matrix which is equivalent to A and whose first row contains entries f_1 and $c_{ij}(x)$. As in Step 1, we see that this is impossible. Hence, f_1 divides every entries of C.

Thus, $f_1(x)$ is the gcd of all 1×1 sub-determinants of B, and hence also the gcd of all 1×1 sub-determinants of A.

Now by induction, C is equivalent to $\mathrm{diag}(f_2(x), \cdots, f_r(x), \mathbf{0})$ where $f_2 | f_2 \cdots | f_r$. Since f_1 divides every entries of C, and therefore the gcd of all 1×1 sub-determinants of C, which is $f_2(x)$. Hence, $f_1 | f_2 \cdots | f_r$, and A is equivalent to

$$S = \mathrm{diag}(f_1(x), \cdots, f_r(x), \mathbf{0}).$$

Since the gcd of all $t \times t$ sub-determinants of S is $\Pi_{i=1}^{t} f_i(x)$, we see that $f_t, \cdots, f_r$ are unique. This proves the theorem. □

Remark 5.1. A complete proof of Lemmas 5.5, 5.6, and Theorem 5.8 goes as follows.

1. Let S be the set of all those that can be written as the product of elementary matrices. Since every elementary matrix has an inverse which is also elementary (cf exercise), every matrix in S has an inverse in S. In addition, every element in S has a non-zero scalar determinant.

2. Define equivalence over $\mathbb{F}[x]$ by $B \sim A$ if $B = PAQ$ for some $P, Q \in S$. Following part of the proof of Theorem 5.8, one can show that for every $A \in M_{m,n}(\mathbb{F}[x])$, there are $P, Q \in S$ such that $PAQ = \mathrm{diag}(f_1, \cdots, f_r, \mathbf{0})$, where $f_1, \cdots, f_r$ are monic polynomials.

3. Suppose $A \in M_n(\mathbb{F}[x])$ has a non-zero scalar determinant. Let $P, Q \in S$ such that $PAQ = \mathrm{diag}(f_1, \cdots, f_n)$. Since $f_1 \cdots f_n = \det(P)\det(A)\det(Q)$ is a non-zero scalar, $f_1 = \cdots = f_n = 1$; that is, $PAQ = I$. Hence, $A = P^{-1}Q^{-1} \in S$. Thus, $A \in S$ if and only if $\det(A)$ is a non-zero scalar.

4. Suppose $A \in M_n(\mathbb{F}[x])$ is invertible, i.e., there exists B such that $AB = BA = I$. Then $1 = \det(A)\det(B)$, so that $\det(A)$ is a non-zero scalar. Thus, $A \in M_n(\mathbb{F})$ *is invertible if and only if* $\det(A)$ *is a non-zero scalar, and if and only if* A *is the product of elementary matrices.*

Since every entries of a matrix A in $M_{m,n}(\mathbb{F}[x])$ is a polynomial, we can express it as

$$A = A_k x^k + \cdots + A_1 x + A_0 x^0 = x^k A_k + \cdots + x^0 A_0, \qquad A_j \in M_{m,n}(\mathbb{F}) \quad \forall j.$$

If $A_m \neq \mathbf{0}$, we say the degree of A is m, writing as $\deg(A) = m$. Also we call A_m the *leading coefficient matrix*.

One can verify that if $B = x^l B_l + \cdots + x^0 B_0$, then, as long as sizes match,

$$\begin{aligned} AB &= \sum_{t=0}^{k+l} x^t C_t = \sum_{t=0}^{k+l} C_t x^t, \quad C_t := \sum_{i+j=t} A_i B_j, \\ BA &= \sum_{t=0}^{k+l} x^t D_t = \sum_{t=0}^{k+l} D_t x^t, \quad D_t := \sum_{i+j=t} B_j A_i. \end{aligned}$$

A square matrix $A \in M_n(\mathbb{F}[x])$ is called a **proper matrix polynomial** if its leading coefficient matrix is invertible. The following lemma shows that a proper matrix polynomial can be used as a divisor.

Lemma 5.7 (Division Algorithm). *Let* $B, D \in M_n(\mathbb{F}[x])$ *and* D *be proper.*

Then **the division of B on the right by D** *has a unique* **right quotient** Q_r *and a unique* **right remainder** R_r*; namely,*

$$B = Q_r D + R_r, \quad \textit{either} \;\; R_r = 0 \;\; \textit{or} \;\; \deg(R_r) < \deg(D).$$

Similarly, the division of B on the left by D has a unique left quotient Q_l and left remainder R_l such that

$$B = DQ_l + R_l, \quad \textit{either} \;\; R_l = 0 \;\; \textit{or} \;\; \deg(R_l) < \deg(D).$$

In particular, if $D = xI - A$ and $\mathbf{B} = \sum_{i=0}^m x^i B_i$ where $A, B_0, \cdots, B_m \in M_n(\mathbb{F})$, then

$$R_r = \mathbf{B}_r(A) := \sum_{i=0}^m B_i A^i, \qquad R_l = \mathbf{B}_l(A) := \sum_{i=0}^m A^i B_i.$$

The proof follows from a long division. Here the condition that D is proper is important.

An important application of the division algorithm is the following:

Corollary 5.2. *Assume that $A_1, A_2, B_1, B_2 \in M_n(\mathbb{F})$ and A_2 is invertible. Define matrix polynomials $M_1, M_2 \in M_n(\mathbb{F}[x])$ by*

$$M_1 = A_1 x + B_1, \qquad M_2 = A_2 x + B_2.$$

Then M_1 is equivalent to M_2 over $\mathbb{F}[x]$ if and only if A_1 is invertible and M_1 and M_2 are equivalent over $\mathbb{F}$, i.e., there exist invertible matrices $P_0, Q_0 \in M_n(\mathbb{F})$ such that

$$M_2 = P_0 M_1 Q_0 \quad \Big(\textit{or } A_2 = P_0 A_1 Q_0, \quad B_2 = P_0 M_1 Q_0 \Big).$$

Proof. We need only show that the only if part. For this, we assume that M_2 is equivalent to M_1 over $\mathbb{F}[x]$. Then there exist invertible $P, Q \in M_n(\mathbb{F}[x])$ such that $M_2 = P M_1 Q$.

Since A_2 is invertible, M_2 is proper, so we can divide P on the left by M_2 and divide Q on the right by M_2 to obtain quotients and remainders as follows:

$$P = M_2 \hat{P} + P_0, \quad Q = \hat{Q} M_2 + Q_0.$$

Since the degree of M_2 is one, P_0 and Q_0 are matrices in $M_n(\mathbb{F})$. We can calculate

$$\begin{aligned}
M_2 &= P M_1 Q = (M_2 \hat{P} + P_0) M_1 (\hat{Q} M_2 + Q_0) \\
&= P_0 M_1 Q_0 + P_0 M_1 \hat{Q} M_2 + M_2 \hat{P} M_1 Q_0 + M_2 \hat{P} M_1 \hat{Q} M_2 \\
&= P_0 M_1 Q_0 + (P - M_2 \hat{P}) M_1 \hat{Q} M_2 + M_2 \hat{P} M_1 (Q - \hat{Q} M_2) + M_2 \hat{P} M_1 \hat{Q} M_2 \\
&= P_0 M_1 Q_0 + P M_1 \hat{Q} M_2 + M_2 \hat{P} M_1 Q - M_2 \hat{P} M_1 \hat{Q} M_2 \\
&= P_0 M_1 Q_0 + M_2 Q^{-1} \hat{Q} M_2 + M_2 \hat{P} P^{-1} M_2 - M_2 \hat{P} M_1 \hat{Q} M_2,
\end{aligned}$$

where we have used $P_0 = P - M_2 \hat{P}$, $Q_0 = Q - \hat{Q} M_2$ in the third equation and $P M_1 = M_2 Q^{-1}$, $M_1 Q = P^{-1} M_2$ in the last equation. Hence,

$$M_2 - P_0 M_1 Q_0 = M_2 D M_2, \qquad D := Q^{-1} \hat{Q} + \hat{P} P^{-1} - \hat{P} M_1 \hat{Q}.$$

We claim that $D = \mathbf{0}I$. Indeed, if $D \neq 0I$, then letting $D_m \neq 0I$ be the leading coefficients of D with $m = \deg(D) \geq 0$, the degree of $M_2 D M_2$ is $m + 2$ since A_2 invertible implies that the leading coefficient matrix $A_2 D_m A_2$ of $M_2 D M_2$ is non-zero. But this is impossible since the degree of $M_2 - P_0 M_1 Q_0$ is at most one. Hence, we must have $D = 0I$.

Thus, $M_2 = P_0 M_1 Q_0$. This equation also implies that $A_2 = P_0 A_1 Q_0$ and $B_2 = P_0 B_1 Q_0$. Since A_2 is invertible, P_0, Q_0 and A_1 are all invertible. This completes the proof. □

Finally we provide an application of matrices over $\mathbb{C}[x]$ to systems of ordinary differential equations with constant coefficients.

Consider a system of 2 ordinary differential equations of 2 unknowns $y_1 = y_1(t), y_2 = y_2(t)$:

$$y_1'' - y_1' + y_2' = 0, \quad y_1' - y_1 + y_2' + y_2 = 0.$$

Introduce a symbol

$$D = ' = \frac{d}{dt}.$$

Then this system can be written as

$$A\mathbf{y} = \mathbf{0}, \quad A = A(D) := \begin{pmatrix} D^2 - D & D \\ D - 1 & D + 1 \end{pmatrix}, \quad \mathbf{y} = \mathbf{y}(t) := \begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix}. \tag{5.2}$$

By elementary row operations, this system is equivalent to

$$D^2 y_2 = 0, \qquad (D+1)y_1 + (D-1)y_2 = 0.$$

Hence, the general solution can be written as

$$y_2 = c_1 + c_2 t, \qquad y_1 = c_1 + 2c_2 + c_2 t + c_3 e^x,$$

where c_1, c_2, c_3 are arbitrary constants.

The general homogeneous system of n linear ordinary differential equations of constant coefficients with n unknowns can be written as

$$A\mathbf{y} = \mathbf{0}, \qquad A = A(D) = \left(a_j^i(D)\right)_{n\times n}, \quad a_j^i(D) = \sum_{k=1}^{m(i,j)} b_{jk}^i D^k, \quad \mathbf{y} = (y^i)_{n\times 1}$$

where b_{jk}^i are constants. The integer $\max\{m(i,j)\}$ is called the order of the system.

By the theorem, A is equivalent to its Smith's canonical form:

$$S = PAQ$$

where P, Q are invertible, and $S = \operatorname{diag}(f_1(D), \cdots, f_r(D), 0, \cdots, 0)$ with $f_1 | f_2 \cdots | f_r$. Hence, setting $\mathbf{z} = Q^{-1}(D)\mathbf{y}$, or $\mathbf{y} = Q(D)\mathbf{z}$, the system then is equivalent to a system of decoupled equations

$$f_1(D)z_1 = 0, \quad \cdots\cdots, \quad f_r(D)z_r = 0. \tag{5.3}$$

Suppose, for example, $f_1(D) = (D-1)^3(D^2+1)(D-2)$, then the general solution of z_1 is

$$z_1(t) = c_1 e^{2t} + c_2 \sin t + c_3 \cos t + (c_4 + c_5 t + c_6 t^2)e^t.$$

Another important application of matrix polynomial will be presented in the next section.

Exercise 33. *Show that every elementary matrix has an inverse which is also elementary.*

Also show that each elementary matrix obtained by performing a single elementary row operation on I can be obtained by performing a single elementary column operation on I, and vice versa.

Exercise 34. *Prove Lemma 5.7.*

Exercise 35. *Find the inverse of the matrices*

$$\begin{pmatrix} x & x+1 \\ x+2 & x+3 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + x^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Also, write these matrices as the product of elementary matrices.

Exercise 36. *Find the Smith's canonical form for the following matrices:*

$$\begin{pmatrix} x & x^2 \\ x^3 & x^5 \end{pmatrix}, \qquad \begin{pmatrix} x & x \\ x^2+x & x \end{pmatrix}$$

Exercise 37. *Show that M_1 and M_2 in Corollary 5.2 are equivalent if and only if $xI + A_1^{-1}B_1$ and $xI + A_2^{-1}B_2$ have the same invariant factors.*

Exercise 38. *If A is a square matrix over $\mathbb{F}[x]$, show that A is equivalent to its transpose.*

Exercise 39. *For the matrix A in (5.2), find invertible $P, Q \in M_n(\mathbb{R}[x])$ such that PAQ is in the Smith canonical form. Also, write the corresponding decoupled system as in (5.3).*

5.7 Similarity

Definition 5.10. *Two square matrices $A, B \in M_n(\mathbb{F})$ are called* **similar** *if $B = P^{-1}AP$ for some invertible $P \in M_n(\mathbb{F})$.*

Definition 5.11. *Let $A \in M_n(\mathbb{F})$ be a square matrix.*

1. *The matrix $xI - A \in M_n(\mathbb{F}[x])$ is called the* **characteristic matrix** *of A. The* **characteristic polynomial** *of A is*
$$p_A(x) = \det(xI - A).$$

2. *If $f \in \mathbb{F}[x]$ satisfies $f(A) = 0I$, we say f* **annihilates** *A. Among all monic polynomials that annihilate A, the one with the minimum degree is unique and, denoted by $m_A(x)$, is called the* **minimum polynomial** *of A.*

3. *Let $f_1, \cdots, f_n$ be the unique monic polynomials such that $f_1|f_2|\cdots|f_n$ and $xI - A$ is equivalent over $\mathbb{F}[x]$ to $\operatorname{diag}(f_1, \cdots, f_n)$. Then $\{f_1, \cdots, f_n\}$ are called the* **similarity invariants** *of A. Those which are not constant are called non-trivial.*

4. *Suppose $f_1, \cdots, f_n$ are similarity invariants of A and*
$$f_j(x) = p_1(x)^{c_{j1}} \cdots p_m(x)^{c_{jm}}, \quad j = 1, \cdots, n.$$
where $c_{ji} \geq 0$ are integers, $p_1(x), \cdots, p_m(x)$ are distinct, monic, irreducible polynomials . Then each non-constant $p_i^{c_{ji}}(x)$ is called an **elementary divisor**, *and all elements in the list, counting duplications,*
$$\{p_i(x)^{c_{ji}} \ ; \ c_{ji} \geq 1\}$$
are called the **elementary divisors** *of A over $\mathbb{F}$.*

We know that similarity is an RST relation. Also,

$$f_1(x) \cdots f_n(x) = \det(xI - A) = d_1(x) \cdots d_m(x),$$

where $\{f_1, \cdots, f_n\}$ are all similarity invariants, and $\{d_1, \cdots, d_m\}$ are all elementary divisors. All trivial similarity invariants of A are equal to unity.

Also, elementary divisors and similarity invariants can be found from one to the other.

Example 5.4. Suppose a 12×12 matrix A has the following similarity invariants

$$f_1(x) = \cdots = f_9(x) = 1, \quad f_{10}(x) = x^2 + 1, \quad f_{11}(x) = (x^2 + 1)(x^2 - 2), \quad f_{12}(x) = (x^2 + 1)(x^2 - 2)^2.$$

Then all elementary divisors of A over $\mathbb{Q}$ are

$$x^2 + 1, \quad x^2 + 1, \quad x^2 + 1, \quad x^2 - 2, \quad (x^2 - 2)^2.$$

All the elementary divisors of A over $\mathbb{C}$ are

$$x + \mathbf{i}, \ x + \mathbf{i}, \ x + \mathbf{i}, \ x - \mathbf{i}, \ x - \mathbf{i}, x - \mathbf{i}, x - \sqrt{2}, \ x + \sqrt{2}, (x - \sqrt{2})^2, \ (x + \sqrt{2})^2.$$

The following theorem shows that similarity invariants and/or elementary divisors are exactly the quantities that are not changed under similarity transformations.

Theorem 5.9. *Let $A, B \in M_n(\mathbb{F})$ be two square matrices over $\mathbb{F}$. The following statements are equivalent:*

1. *B is similar to A over $\mathbb{F}$, i.e., there exist invertible $P \in M_n(\mathbb{F})$ such that $B = P^{-1}AP$;*
2. *$xI - B$ and $xI - A$ are equivalent over $\mathbb{F}$;*
3. *$xI - B$ and $xI - A$ are equivalent over $\mathbb{F}[x]$; i.e, there exist invertible $P, Q \in M_n(\mathbb{F}[x])$ such that*

$$xI - B = P\ (xI - A)\ Q\ ;$$

4. *Both A and B have the same similarity invariants;*
5. *Both A and B have the same elementary divisors over $\mathbb{F}$;*
6. *For each $i = 1, \cdots, n$, the* gcd *of all $i \times i$ sub-determinants of $xI - B$ equals that of $xI - A$.*
7. *A is similar to B over $\mathbb{K}$ where $\mathbb{K}$ is a field containing $\mathbb{F}$.*

Proof. (1)⇒(2). If $B = P^{-1}AP$, then $xI - B = P^{-1}(xI - A)P$ so that $xI - B$ is equivalent to $xI - A$ over $\mathbb{F}$.

(2) ⇒ (3) is trivial, since invertible matrices in $M_n(\mathbb{F})$ are also invertible matrices in $M_n(\mathbb{F}[x])$.

(3) ⇒ (1). Suppose $xI - B$ is equivalent to $xI - A$ over $\mathbb{F}[x]$. Then by Corollary 5.2, $xI - B$ is equivalent to $xI - A$ over $\mathbb{F}$, i.e. there exist invertible $P_0, Q_0 \in M_n(\mathbb{F})$ such that $xI - A = P_0(xI - B)Q_0$. This implies that $I = P_0Q_0$ and $A = P_0BQ_0$, i.e. $B = P_0^{-1}AP_0$. Hence, B is similar to A.

Finally, the equivalence of (3),(4),(5),(6),(7) follows from Theorem 5.8 and the definitions of similarity invariants and elementary divisors, and Theorem 5.7. □

Note that if a non-trivial polynomial f annihilates A, $f(A) = 0I$, then so is the $\gcd[m_A, f]$ since it is a linear combination of m_A and f. As m_A has minimum degree, we must have $m_A = \gcd[m_A, f]$, i.e. $m_A | f$. Hence, the minimum polynomial of A is the gcd of all non-trivial polynomials that annihilate A.

Theorem 5.10. *The minimum polynomial $m_A(x)$ of a square matrix $A \in M_n(\mathbb{F})$ is that similarity invariant of A that has the highest degree.*

That is, if $f_1, \cdots, f_n$ are invariant factors of $xI - A$ over $\mathbb{F}[x]$ where $f_1 | f_2 | \cdots | f_n$, then $f_n(x)$ is the minimum polynomial; in particular,

$$m_A(x) = \frac{p_A(x)}{g_{n-1}(x)}$$

where $p_A(x) = \det(xI - A)$ and $g_{n-1}(x)$ is the gcd *of all $(n-1) \times (n-1)$ sub-determinants of $(xI - A)$.*

Proof. Denote by $Q = Q(x)$ the adjoint of $xI - A$. Then

$$(xI - A)Q = p_A(x)I.$$

Since the entries of Q consist of all $(n-1) \times (n-1)$ sub-determinants of $xI - A$, and $g_{n-1}(x)$ is the gcd of all $(n-1) \times (n-1)$ sub-determinants of $xI - A$, we see that g_{n-1} divides every entries of Q, so that we can write $Q = g_{n-1}\hat{Q}$, and the gcd of all entries of $\hat{Q}$ is 1.

Hence,

$$g_{n-1}(xI - A)\hat{Q} = p_A I = g_{n-1} f_n I.$$

Therefore,

$$f_n I = (xI - A)\hat{Q}$$

Now applying the in particular part of Lemma 5.7 with $D = xI - A$ and $B = f_n(x)I$ we conclude that the left remainder of B divided by D on the left is $0I$, i.e, $f_n(A)I = 0I$. Hence, $m_A | f_n$. We write $f_n(x) = m_A(x)h(x)$ where h is a monic polynomial.

Again using the division algorithm Lemma 5.7 for the division of $m_A(x)\mathbf{I}$ on the left by $xI - A$ we have left remainder $m_A(A)I = 0I$. Hence, denote by $H(x)$ the left quotient, we have

$$m_A(x)\mathbf{I} = (xI - A)H(x).$$

It the follows that

$$(xI - A)\hat{Q}(x) = f_n(x)I = h(x)m_A(x)I = h(x)(xI - A)H(x),$$

or

$$\hat{Q}(x) = h(x)H(x).$$

From this, we see that $h(x)$ is a common divisor of all enteries of $\hat{Q}$, which has to be a constant. As h is monic, $h = 1$ and $f_n(x) = m_A(x)$. □

So far we have established necessary and sufficient conditions for matrices to be similar. Next, we study canonical forms under similarity transformations. For this, we first study a special kind of matrices whose invariants can be easily calculated.

Definition 5.12. *Let $n \geq 1$ and q be a monic polynomial in the form*

$$q(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0 \ .$$

(1) The **companion matrix** *of q is defined by, when $n \geq 2$,*

$$C(q) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \end{pmatrix}_{n\times n},$$

When $n = 1$ so that $q(x) = x - a_0$, we defined $C(q) := (a_0)$.

(2) For any integer $e \geq 2$, the **hyper-companion matrix** *of q^e is*

$$C_e(q) := \begin{pmatrix} C(q) & N & 0 & \cdots & 0 \\ 0 & C(q) & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & N \\ 0 & 0 & 0 & \cdots & C(q) \end{pmatrix}_{(en)\times(en)}$$

where N is a $n \times n$ matrix whose entries are all zero except the one at the lower left-hand corner, which is 1. When $e = 1$, $C_e(q) := C(q)$.

Lemma 5.8. *Let $q \in \mathbb{F}[x]$ be a monic polynomial of degree $n \geq 1$. Then*

(1) both the characteristic and minimum polynomials of the companion matrix $C(q)$ are equal to $q(x)$;

(2) both the characteristic and minimum polynomials of the hyper-companion matrix $C_e(q)$ are equal to $q^e(x)$.

That is, for $e \geq 1$, the similarity invariants of $C_e(q)$ are $\{1, \cdots, 1, q^e(x)\}$, and $C_e(q)$ has only one elementary divisor, being $q^e(x)$.

Proof. Direct calculation shows that the characteristic polynomial of $C(q)$ is q and that of $C_e(q)$ is $q(x)^e$.

Since the determinant of the submatrix obtained by deleting the first column and last row of $C(q) - xI$ is 1, the gcd of all $(n-1) \times (n-1)$ sub-determinants of $xI - C(g)$ is 1. Theorems 5.10 and 5.8 imply that the minimum polynomial of $C(g)$ equals its characteristic polynomial.

One observes that $C_e(q)$ has just above its diagonal an unbroken line of elements equal to 1. All elements above this line are zero. Hence, $xI - C_e(q)$ contains a sub-matrix whose determinant equals that of $-I_{ne-1}$. Thus, the gcd of all $(ne-1) \times (ne-1)$ sub-determinants of $xI - C_e(q)$ is 1, and the assertion of the lemma follows. □

Our goal is to find canonical forms that is "as much as" diagonal as possible. For this, we point out the following facts:

Suppose

$$B = \text{diag}(B_1, \cdots, B_r), \quad C = \text{diag}(C_1, \cdots, C_r), \quad P = \text{diag}(P_1, \cdots, P_r)$$

where for each $i = 1, \cdots, r$, B_i, C_i, P_i are square matrices of same size and P_i invertible. We say that B is a **direct sum** of $B_1, \cdots, B_r$. Note that P is invertible, and

$$\begin{aligned} BC &= \text{diag}(B_1C_1, \cdots, B_rC_r), \\ P^{-1} &= \text{diag}(P_1^{-1}, \cdots, P_r^{-1}), \\ P^{-1}BP &= \text{diag}(P_1^{-1}B_1P_1, \cdots, P_r^{-1}B_rP). \end{aligned}$$

Using these facts, we can prove the following:

Lemma 5.9. *1.* **Similarity of Direct Sums:**

If B_i is similar to C_i for $i = 1, \cdots, r$, then $\text{diag}(B_1, \cdots, B_r)$ *is similar to* $\text{diag}(C_1, \cdots, C_r)$.

2. **Equivalence of Direct Sums:**

If B_i is equivalent over $\mathbb{F}[x]$ to C_i for all $i = 1, \cdots, r$, then $\text{diag}(B_1, \cdots, B_r)$ *is equivalent over $\mathbb{F}$ to* $\text{diag}(C_1, \cdots, C_r)$.

3. **Shuffling:**

Suppose for $i = 1, \cdots, r$, B_i is a square matrix over $\mathbb{F}[x]$. Then for any permutation p of r indexes, $\text{diag}(B_1, \cdots, B_r)$ *is equivalent over $\mathbb{F}$ to* $\text{diag}(B_{p(1)}, \cdots, B_{p(r)})$.

4. **Decomposition:**

Suppose $\gcd[f(x), g(x)] = 1$. *Then* $\text{diag}(1, fg)$ *is equivalent over $\mathbb{F}[x]$ to* $\text{diag}(f, g)$. *Similarly, if $q_1, \cdots, q_k$ are pairwise prime to each other, then* $\text{diag}(q_1, \cdots, q_k)$ *is equivalent over $\mathbb{F}[x]$ to* $\text{diag}(I_{k-1}, q_1 \cdots q_k) = \text{diag}(1, \cdots, 1, q_1 \cdots q_k)$.

We are ready to prove the following canonical forms under similarity transformations.

Theorem 5.11. *Every square matrix over $\mathbb{F}$ is similar to*

(1) the direct sum of the companion matrices of non-trivial similarity invariants,

(2) the direct sum of the companion matrices of its elementary divisors over $\mathbb{F}$, and

(3) the direct sum of the hyper-companion matrices of its elementary divisors over $\mathbb{F}$.

That is, for $A \in M_n(\mathbb{F})$, if its non-trivial similarity invariants are $f_k, \cdots, f_n$, elementary divisors over $\mathbb{F}$ are $d_1 = q_1^{e_1}, \cdots, d_m = q_m^{e_m}$ where $q_1, \cdots, q_m$ are irreducible polynomials, then A is similar to the following matrices:

$$\begin{gathered}\operatorname{diag}\Big(C(f_k), \cdots, C(f_n)\Big),\\ \operatorname{diag}\Big(C(d_1), \cdots, C(d_m)\Big),\\ \operatorname{diag}\Big(C_{e_1}(q_1), \cdots, C_{e_m}(q_m)\Big).\end{gathered}$$

Proof. 1. We know that if $t = \deg(f)$, then $xI - C(f)$ has invariant factors $\{1, \cdots, 1, f\}$, so that $xI_t - C(f)$ is equivalent over $\mathbb{F}[x]$ to $\operatorname{diag}(I_{t-1}, f) = \operatorname{diag}(1, \cdots, 1, f)$.

Denote $t_i = \deg(f_i)$. Then over $\mathbb{F}[x]$, the matrix $xI - \operatorname{diag}(C(f_k), \cdots, C(f_n)) = \operatorname{diag}\Big([xI_{t_k} - C(f_k)], \cdots, [xI_{t_n} - C(f_n)]\Big)$ is equivalent to

$$\operatorname{diag}\Big(\operatorname{diag}(1, \cdots, 1, f_k),\ \cdots, \operatorname{diag}(1, \cdots, 1, f_n)\Big)$$

which after shuffling, is equivalent to $\operatorname{diag}(1, \cdots, 1, f_k, \cdots, f_n)$, which, by the definition of invariant factors, is equivalent to $xI - A$. Hence, A is similar to $\operatorname{diag}(C(f_k), \cdots, C(f_n))$.

2. Any non-trivial similarity invariant f can be written as $f = p_1 \cdots p_s$ where $p_1, \cdots, p_s$ are elementary divisors and are pairwise prime to each other. Denote by n_i the degree of p_i and by t the degree of f. Then over $\mathbb{F}[x]$, the polynomial matrix $xI_t - C(f)$ is equivalent to

$$\operatorname{diag}(1, \cdots, 1, f) = \operatorname{diag}(1, \cdots, 1, p_1, \cdots, p_s),$$

which, by decomposition and shuffling, , is equivalent to

$$\operatorname{diag}\Big(\operatorname{diag}(1, \cdots, 1, p_1),\ \cdots, \operatorname{diag}(1, \cdots, 1, p_s)\Big),$$

which is equivalent to

$$\operatorname{diag}([xI_{n_1} - C(p_1)],\ \cdots, [xI_{n_s} - C(p_s)]\Big) = xI_t - \operatorname{diag}(C(p_1), \cdots, C(p_s)).$$

Hence, $C(f)$ is similar to $\operatorname{diag}(C(p_1), \cdots, C(p_s))$. It then follows, by the similarity of direct sums and shuffling, that $\operatorname{diag}(C(f_k), \cdots, C(f_n))$ is similar to $\operatorname{diag}(C(d_1), \cdots, C(d_m))$.

3. Since both the similarity invariants of $C(q_i^{e_i})$ and that of $C_{e_i}(q_i)$ are equal to $\{1, \cdots, 1, q_i^{e_i}\}$, $C(q_i^{e_i})$ is similar to $C_{e_i}(q_i)$. Hence $\operatorname{diag}\Big(C(d_1), \cdots, C(d_m)\Big)$ is similar to $\operatorname{diag}\Big(C_{e_1}(q_1), \cdots, C_{e_m}(q_m)\Big)$. □

Example 5.5. *Suppose the elementary divisors of $A \in M_5(\mathbb{Q})$ are*

$$x^2 - 2, \quad x - 1, \quad (x-1)^2.$$

Then its similarity invariants are $(x-1)$ and $(x^2-2)(x-1)^2 = x^4 - 2x^3 - x^2 + 4x - 2$. Then matrix $xI - A$ is equivalent over $\mathbb{F}[x]$, for any field $\mathbb{F}$ containing $\mathbb{Q}$, to

$$\operatorname{diag}(x-1, 1, 1, 1, x^4 - 2x^3 - x^2 + 4x - 2) \quad \textit{and} \quad \operatorname{diag}(x-1, 1, (x-1)^2, 1, x^2 - 2).$$

It is equivalent over $\mathbb{R}[x]$ to

$$\operatorname{diag}(x - \sqrt{2}, x + \sqrt{2}, x - 1, 1, (x-1)^2).$$

Hence, over any field containing $\mathbb{Q}$,, A is similar to the following matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & -4 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix}$$

Over $\mathbb{R}$, it is similar to

$$\begin{pmatrix} \sqrt{2} & 0 & 0 & 0 & 0 \\ 0 & -\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

Example 5.6. *Suppose $q = x - a$ is linear. Then $C(q) = (a)$ so that*

$$C_e(q) = \begin{pmatrix} a & 1 & 0 & \cdots & 0 & 0 \\ 0 & a & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a & 1 \\ 0 & 0 & 0 & \cdots & 0 & a \end{pmatrix} =: J_e(a)$$

is indeed a Jordan block.

In particular when $\mathbb{F} = \mathbb{C}$, the canonical form of the direct sum of hyper-companion matrices of elementary divisors stated in the Theorem is in fact the Jordan form.

Example 5.7. *Suppose $\mathbb{F} = \mathbb{R}$ and $q = x^2 - bx - c$ with $b^2 + 4c < 0$ so that q irreducible. Then $C(q) = \begin{pmatrix} 0 & 1 \\ c & b \end{pmatrix}$. For $e = 3$,*

$$C_3(q) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ c & b & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & c & b & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & c & b \end{pmatrix}, \quad C(q^3) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ c^3 & 3bc^2 & 3c(b^2-1) & b^3 - 6bc & 3(c - b^2) & 3b \end{pmatrix}$$

Example 5.8. *Suppose $\mathbb{F} = \mathbb{R}$ and $q(x) = (x - \lambda)(x - \bar{\lambda})$ where $\lambda = \alpha + \mathbf{i}\beta$, $\beta > 0, \alpha \in \mathbb{R}$. Consider*

$$C = C(\alpha, \beta) := \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}_{2\times 2}, \qquad C_k = C_k(\alpha, \beta) := \begin{pmatrix} C & I & 0 & \cdots & 0 & 0 \\ 0 & C & I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & C & I \\ 0 & 0 & 0 & \cdots & 0 & C \end{pmatrix}_{(2k)\times(2k)}.$$

Then $\det(xI - C) = q$, and since $\beta > 0$, $xI - C$ is equivalent over $\mathbb{R}[x]$ to $\operatorname{diag}(1, q)$. Also, $\det(xI - C_k) = (\det(xI_2 - C))^k = q^k$. Hence, the minimum polynomial of C_k is q^l for some integer $l \leq k$. One can calculate $q(C) = 0I_2$ and

$$q(C_k) = \begin{pmatrix} 0 & 2\beta E & I & & 0 \\ & \ddots & \ddots & \ddots & \\ & & 0 & 2\beta E & I \\ & & & 0 & 2\beta E \\ 0 & & & & 0 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

It is then easy to calculate that

$$q(C_k)^{k-1} = \begin{pmatrix} 0 & (2\beta E)^{k-1} \\ 0I_{2(k-1)} & 0 \end{pmatrix} \neq 0I.$$

Thus, the minimum polynomial of C_k is q^k. Hence, the companion matrix $C(q^k)$ is similar to the real Jordan matrix $C_k(\alpha, \beta)$. From this, we obtain the real Jordan canonical form.

Corollary 5.3. *Every square complex matrix is similar to a Jordan form*

$$\operatorname{diag}\Big(J_{e_1}(\lambda_1), \cdots, J_{e_m}(\lambda_m)\Big).$$

Every square real matrix is similar over $\mathbb{R}$ to a real Jordan form

$$\operatorname{diag}\Big(J_{e_1}(\lambda_1), \cdots, J_{e_k}(\lambda_k), C_{e_{k+1}}(\alpha_{k+1}, \beta_{\beta_{k+1}}), \cdots, C_{e_m}(\alpha_m, \beta_m)\Big)$$

where λ_i, $i = 1, \cdots, k$ are real eigenvalues, and $\alpha_j + \beta_j \mathbf{i}$ are complex eigenvalues.

Finally, we provide a criteria for a matrix to be similar to a diagonal matrix.

Theorem 5.12. *A square matrix $A \in M_n(\mathbb{F})$ is similar (over $\mathbb{F}$) to a diagonal matrix if and only if all of its elementary divisors over $\mathbb{F}$ are linear, and also if and only if its minimum polynomial can be written as a product of distinct linear polynomials.*

Exercise 40. *Find the similarity invariants and elementary divisors of the following matrices*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Exercise 41. *Show that all elementary divisors determine uniquely all similarity invariants, and vice versa.*

Exercise 42. *Prove Lemma 5.9*

Exercise 43. *Show that the characteristic polynomial of the companion matrix $C(q)$ is q, and the characteristic polynomial of the hyper-companion matric $C_e(q)$ is q^e.*

Exercise 44. *Show that for every polynomial q and integer $e \geq 2$, the companion matrix $C(q^e)$ and hyper-companion matrix $C_e(q)$ are similar.*

Exercise 45. *Let $A \in M_n(\mathbb{F})$. Assume that both its minimum polynomial and characteristic polynomial are equal to $p(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$. Show that there is a vector $\mathbf{u} \in \mathbb{F}^n$ such that*

$$\{\mathbf{u}, A\mathbf{u}, \cdots, A^{n-1}\mathbf{u}\}$$

is a basis of $\mathbb{F}^n$. In addition, under this basis, the matrix of the linear map $\mathbf{Ax} := A\mathbf{x}$ is

$$C(p)^T := \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n-2} \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}$$

Exercise 46. *(1) Show that given any set of non-trivial monic polynomials $g_1, \cdots, g_k$ satisfying $g_1|g_2 \cdots |g_k$, there exists a matrix $A \in M_n(\mathbb{F})$, where $n = \sum_i \deg(g_i)$, such that $g_1, \cdots, g_k$ are exactly the non-trivial similarity invariants of A.*

(2) Show that given any set of non-constant monic polynomials $d_1(x), \cdots, d_m(x)$, there is a square matrix whose elementary divisors are exactly $d_1, \cdots, d_m$.

Exercise 47. *Prove Theorem 5.12.*

Exercise 48. *Find a matrix in (i) $M_n(\mathbb{Q})$, (ii) in $M_n(\mathbb{R})$, and (iii) in $M_n(\mathbb{C})$ such that it has the following set of non-trivial similarity invariants:*

(1) $x-1, x^2-2, x^2+1$;

(2) $x-1, (x-1)^2$;

(3) $x^2-2, (x^2+1)^2$.

5.8 Orthogonal and Unitary Similarity

Definition 5.13. *1. A real square matrix O is called* **orthogonal** *if $O^TO = I$.*

2. The adjoint A^* of a complex matrix A is $A^* = \bar{A}^T$.

3. A complex square matrix U is called **unitary** *if $U^*U = I$.*

4. Two matrices $A, B \in M_n(\mathbb{R})$ are called **orthogonally similar** *if $B = O^{-1}AO$ where O is an orthogonal matrix.*

5. Two matrices $A, B \in M_n(\mathbb{C})$ are called **unitarily similar** *if $B = U^{-1}AU$ where U is a unitary matrix.*

6. A complex matrix A is called **normal** *if $A^*A = AA^*$.*

Note that an orthogonal matrix is also a unitary matrix, and a unitary matrix is orthogonal if and only it is real. Also, orthogonal similarity implies simultaneously similarity and congruence, whereas unitary similarity implies simultaneously similarity and Hermitian congruence.

We shall focus our attention to matrices that can be diagonalized.

Theorem 5.13. *1. A real square matrix is orthogonally similar to a diagonal matrix if and only it is symmetric.*

2. A complex matrix is unitarily similar to a real diagonal matrix if and only if it is Hermitian.

3. A complex matrix is unitarily similar to a diagonal matrix if and only if it is normal.

4. If A is real and normal, then A is orthogonally similar to

$$\operatorname{diag}(\lambda_1, \cdots, \lambda_r, C_{r+1}, \cdots, C_t)$$

where $\lambda_1, \cdots, \lambda_r$ are real eigenvalues of A and

$$C_j = \begin{pmatrix} \alpha_j & \beta_j \\ -\beta_j & \alpha_j \end{pmatrix}$$

where $\alpha_j + \mathbf{i}\beta_j$, $j = r+1, \cdots, m$, are complex eigenvalues of A.

Note that a real diagonal matric is both symmetric and Hermitian. A complex diagonal matrix is normal. A diagonal matrix is Hermitian if and only if it real. Also, real symmetry and normality are both preserved under orthogonal similarity transformation $A \to O^{-1}A$, and normality and Hermitian are both preserved under unitary similarity transformation $A \to U^{-1}AU$. Hence, the only if parts of the statements are easy to verify.

We now prove the if part. Since real symmetric and complex Hermitian matrices are normal matrices, we only focus our attention on normal matrices.

Hence, suppose A is a normal matrix. Denote by m the characteristic polynomial of A. Let λ be an eigenvalue of A. We claim that $m(x) = (x - \lambda)g(x)$ where $g(\lambda) \neq 0$. Suppose this is not true. Then we can write

$$g(x) = (x - \lambda)h(x), \quad m(x) = (x - \lambda)^2 h(x).$$

Since $g(A)$ is a non-zero matrix, there exists $\eta \in \mathbb{C}^n$ such that $\xi := g(A)\eta \neq 0$. Hence,

$$(\lambda I - A)\xi = m(A)\eta = 0.$$

Namely, ξ is an eigenvector of A. We claim that it is also an eigenvector of A^*. Indeed,

$$\|(\bar{\lambda} - A^*)\xi\|^2 = ((\bar{\lambda} - A^*)\xi)^*((\bar{\lambda}I - A^*)\xi)) = \xi^*(\lambda I - A)(\bar{\lambda}I - A^*)\xi = \xi^*(\bar{\lambda}I - A^*)(\lambda I - A)\xi = 0,$$

since $A^*A = AA^*$ implies $(\lambda I - A)(\bar{\lambda}I - A^*) = (\bar{\lambda}I - A^*)(\lambda I - A)$. We then calculate,

$$\|\xi\|^2 = \xi^*\xi = \xi^* g(A)\eta = \xi^*(\lambda I - A)h(A)\eta = ((\bar{\lambda}I - A^*)\xi)^* h(A)\eta = 0,$$

which is impossible.

Hence $m(x) = (x - \lambda)h(x)$ where $h(\lambda) \neq 0$. Working on each eigenvalue, we then conclude that $m(x)$ is the product of distinct linear polynomials. Consequently, all elementary divisors of A are linear. Thus A is similar to a diagonal matrix. This implies that A has n linearly independent eigenvectors. (The column vectors of P where $P^{-1}AP$ is diagonal).

Let $\lambda_1, \cdots, \lambda_r$ be all distinct eigenvalues of A, with multiplicity $m_1, \cdots, m_r$ respectively. Then the eigenspace for λ_i is m_i dimension, and we can select orthonormal vectors $\{\xi_{i1}, \cdots, \xi_{im_i}\}$ expanding the eigenspace associated with λ_i.

We now show that eigenvectors corresponding to different eigenvalues are orthogonal. Indeed, if (λ, ξ) and (μ, η) are two eigenpairs where $\lambda \neq \mu$, then since $(\bar{\lambda}, \xi)$ is an eigenpair of A^*, we have

$$\mu\xi^*\eta = \xi^* A\eta = (A^*\xi)^*\eta = (\bar{\lambda}\xi)^*\eta = \lambda\xi^*\eta.$$

This implies that $\xi^*\eta = 0$ so that $\xi \perp \eta$.

Hence, $\{\xi_{11}, \cdots, \xi_{1m_1}, \cdots, \xi_{r1}, \cdots, \xi_{rm_r}\}$ is an orthonormal basis of $\mathbb{C}^n$. Consequently, $U := (\xi_{11} \cdots \xi_{1m_1} \cdots \xi_{r1} \cdots \xi_{rm_r})$ is a unitary matrix, and $AU = U\text{diag}(\lambda_1 I_{m_1}, \cdots, \lambda_r I_{m_r})$. Thus, A is unitarily similar to a diagonal matrix.

Finally we consider the case that A is real and normal. As A is normal, we can see that for each eigenvalue λ of multiplicity k, the eigenspace (in $\mathbb{C}^n$) associated with λ is k-dimension. In addition, eigenvectors associated with different eigenvalues are orthogonal to each other.

1. Suppose λ is real. Then the rank of $\lambda I - A$ is $n - k$ (since it has k linearly independent solutions in $\mathbb{C}^n$), so that $(\lambda I - A)\mathbf{x} = 0$ has k linearly independent real solutions. Hence, we can find an orthonormal real basis for the eigenspace of A associated with λ.

2. Suppose $\lambda = \alpha + \mathbf{i}\beta$ ($\beta > 0$). Let $\{\xi_1, \cdots, \xi_k\}$ be an orthognormal basis of the eigenspace. For each ξ in the set, write $\xi = x + \mathbf{i}y$. Since A is normal, we have $A^*\xi = \bar{\lambda}\xi$. As A is real, we obtain from $A\xi = \lambda\xi$ and $A^*\xi = \bar{\lambda}\xi$ that

$$Ax = \alpha x + \beta y, \quad Ay = -\beta x + \alpha y, \qquad A^*x = \alpha x - \beta y, \quad A^*y = \beta x + \alpha y.$$

Thus, using $y^*Ay = y^TAy = (y^TAy)^T = y^TA^Ty = y^*A^*y$ we obtain

$$-\beta y^*x + \alpha y^*y = \beta y^*x + \alpha y^*y.$$

This implies $y^*x = 0$, i.e., $x \perp y$. Similarly, from $x^*Ay = (x^*Ay)^* = y^*A^*x$ we obtain

$$-\beta x^*x + \alpha x^*y = \alpha y^*x - \beta y^*y.$$

This implies that $\|x\| = \|y\|$.

Hence, writing $\xi_i = x_i + \mathbf{i}y_i$, we have $x_i \perp y_i$ and $\|x_i\|^2 = \|y_i\|^2 = 1/2$.

Suppose $i \neq j$. By choice, we have $\xi_i \perp \xi_j$. Since $\bar{\xi}_i$ is an eigenvector of A associated with eigenvalue $\bar{\lambda} \neq \lambda$, we have $\bar{\xi}_i \perp \xi_j$. Hence, ξ_j is orthogonal to $\frac{1}{2}(\xi_i + \bar{\xi}_i) = x_i$ and also to $\frac{1}{2\mathbf{i}}(\xi_i + \bar{\xi}_i) = y_i$ Thus, $0 = \xi_j^* x_i = \xi_j^* y_i$, which implies that $x_j \perp x_i, y_j \perp x_i$, $x_j \perp y_i, y_j \perp y_i$.

Thus, $\{\sqrt{2}x_1, \sqrt{2}y_1, \cdots, \sqrt{2}x_k, \sqrt{2}y_k\}$ is an orthonormal basis for the direct sum of the eigenspaces associated with λ and $\bar{\lambda}$. Under this base, the matrix of the mapping $x \to Ax$ is $\text{diag}(C, \cdots, C)$.

Working for each eigenspace, we then conclude that we can find a real orthonoamal basis

$$\{\xi_1, \cdots, \xi_r, x_1, y_1, \cdots, x_t, y_t\}$$

such that under this basis, the matrix of the mapping $x \to Ax$ is $D = \text{diag}(\lambda_1, \cdots, \lambda_r, C_1, \cdots, C_t)$; namely, set $O = (\xi, \cdots \xi_r\ x_1\ y_1 \cdots x_t\ y_t)$ we have O is orthogonal and $AO = OD$ or $D = O^{-1}AO$. □

Exercise 49. *Show that an orthogonal matrix is a unitary matrix, and a unitary matrix is orthogonal if and only it is real.*

Exercise 50. *Show that the following matrices are normal: the real symmetric matrices, the Hemitian matrices, the real orthogonal matrices, the unitary matrices, the real skew-symmetric matrices, the skew-Hermitian matrices, all matrices unitarily similar to normal matrices.*

Exercise 51. *Suppose that A is a square complex matrix having the property that if (λ, ξ) is an eigenpair of A, then $(\bar{\lambda}, \xi)$ is an eigenpair of A^*. Show that A is unitarily similar to a diagonal matrix, and hence, A is normal.*

Exercise 52. *Show the following:*

(i) If P is positive definite, then there exists a unique positive definite matrix R such that $P = R^2$.

(2) If A is invertible, then there is a unique **polar decomposition**

$$A = RU$$

such that R is positive definite and U is unitary. (Hint: Notice that $AA^* = RUU^*R^* = RR^* = R^2$, so $R = \sqrt{AA^*}$, and $U = R^{-1}A$.)

Exercise 53. *(1) Show that any unitary matrix is unitarily similar to*

$$\text{diag}(e^{\mathbf{i}\theta_1}, \cdots, e^{\mathbf{i}\theta_n})$$

where $0 \leq \theta_i < 2\pi$.

(2) Show that any orthogonal matrix is orthogonally similar to

$$\text{diag}(I_p, -I_q, C_1, \cdots, C_r)$$

where $C_i = \begin{pmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \sin\theta_i \end{pmatrix}$, $\theta_i \in [0, 2\pi)$.