Lecture in Application of Linear Algebra

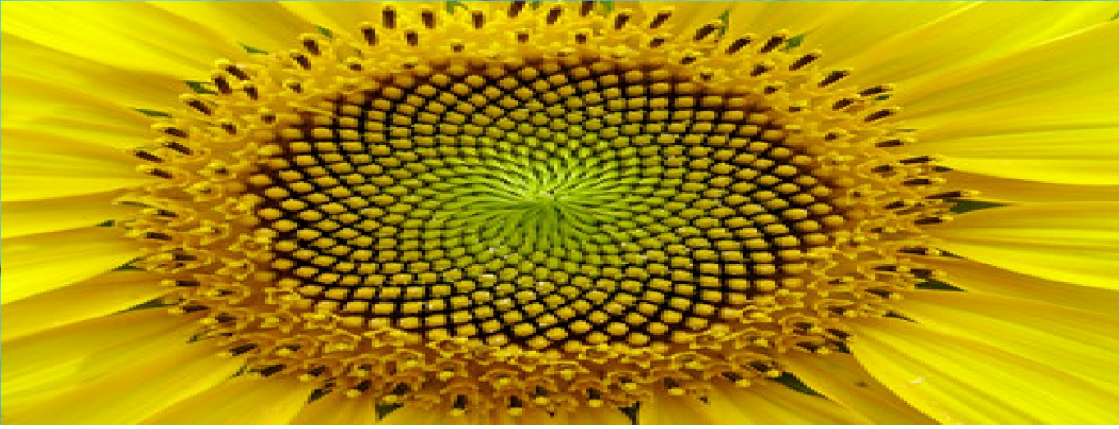
Preparing by

Dr. Amr M. Elrawy

Department of Mathematics, Faculty of Science, South Valley University

Preparing by Dr. Amr M. Elrawy

First release, 2021



Contents

Part I

Topics in Linear Algebra

1. Linear transformations

The central objective of linear algebra is the analysis of linear functions defined on a finite-dimensional vector space.In this chapter, we define the concept of a linear function or transformation.

Definition 1.0.1 Let V and W be real vector spaces (their dimensions can be different), and let T be a function with domain V and range in W (written $T : V \to W$). We say T is a linear transformation if
(i) For all $\mathbf{x}, \mathbf{y} \in V, T(\mathbf{x}+\mathbf{y}) = T(\mathbf{x}) + T(\mathbf{y})$ (T is additive)
(ii) For all $\mathbf{x} \in V, r \in \mathbb{K}, T(r\mathbf{x}) = rT(\mathbf{x})$ (T is homogeneous).

R If $V = W$, then T can be called a linear operator.

R The homogeneity and additivity properties of a linear transformation $T : V \to W$ can be used in combination to show that if $\mathbf{x}$ and $\mathbf{y}$

are vectors in V and r and s are any scalars, then

$$T(r\mathbf{x}+s\mathbf{y}) = rT(\mathbf{x})+sT(\mathbf{y}).$$

■ **Example 1.1** Show that $T : R^2 \to R^2$, defined by

$$T((x_1,x_2)) = (x_1+x_2, x_1-x_2)$$

is a linear transformation.
Solution:
Let $u = (x_1,x_2)$, $v = (y_1,y_2) \in R^2$, then

$$\begin{aligned}(i)T(u+v) &= T((x_1+y_1,x_2+y_2))\\ &= (x_1+y_1+x_2+y_2, x_1+y_1-x_2-y_2)\\ &= (x_1+x_2,x_1-x_2)+(y_1+y_2,y_1-y_2)\\ &= T(u)+T(v).\\ (ii)T(ru) &= T(r(x_1,x_2+y))\\ &= (rx_1+rx_2, rx_1-rx_2)\\ &= r(x_1+x_2,x_1-x_2).\\ &= rT(u).\end{aligned}$$

Therefore, T is linear transformation. ■

■ **Example 1.2** Show that $T : R^2 \to R^2$, defined by

$$T((x_1,x_2)) = (x_1+x_2, x_1-x_2+1)$$

is not linear transformation.
Solution: let $(0,0),(1,1) \in R^2$, then

$$T((0,0)+(1,1)) = T(1,1) = (2,1) \neq (2,2).$$

Therefore, T is not linear transformation. ■

Theorem 1.0.1 If $T : V \to W$ is a linear transformation, then:
(a) $T(\mathbf{0}) = \mathbf{0}$.
$(b)T(\mathbf{u}-\mathbf{v}) = T(\mathbf{u})-T(\mathbf{v})$ for all $\mathbf{u}$ and $\mathbf{v}$ in V.

Proof. Let $\mathbf{u}$ be any vector in V. Since $0\mathbf{u} = \mathbf{0}$, it follows from the homogeneity property in Definition 1 that

$$T(\mathbf{0}) = T(0\mathbf{u}) = 0T(\mathbf{u}) = \mathbf{0}$$

which proves (a) We can prove part (b) by rewriting $T(\mathbf{u}-\mathbf{v})$ as

$$\begin{aligned} T(\mathbf{u}-\mathbf{v}) &= T(\mathbf{u}+(-1)\mathbf{v}) \\ &= T(\mathbf{u})+(-1)T(\mathbf{v}) \\ &= T(\mathbf{u})-T(\mathbf{v}) \end{aligned}$$

We leave it for you to justify each step. ■

■ **Example 1.3** Show that $T : V \to W$, defined by $T(v) = 0$ for every v in V is a linear transformation called the **zero transformation**.
Solution:

$$T(u+v) = 0,\ T(u) = 0,\ T(v) = 0, \text{ and } T(ku) = 0.$$

Therefore,

$$T(u+v) = T(u)+T(v) \text{ and } T(ku) = kT(u).$$

■

■ **Example 1.4** Show that $T : V \to V$, defined by $T(v) = v$ for every v in V is a linear transformation called the **identity operator** on V.
Solution:

$$T(u+v) = u+v,\ T(u) = u,\ T(v) = v, \text{ and } T(ku) = ku.$$

Therefore,

$$T(u+v) = T(u)+T(v) \text{ and } T(ku) = kT(u).$$

■

■ **Example 1.5** Show that $T : V \to V$, defined by $T(v) = kv$ for every v in V and k any scalar is a linear transformation.
Solution:

$$T(u+v) = k(u+v) = ku+kv = T(u)+T(v),$$

and,

$$T(ru) = k(ru) = rku = rT(u).$$

■

R In the above Example 1.5. If $0 < k < 1$, then T is called **the contraction** of V with factor k, and if $k > 1$, it is called **the dilation** of V with factor k.

■ **Example 1.6** Let M_{nn} be the vector space of $n \times n$ matrices. In each part determine whether the transformation is linear.
(a) $T_1(A) = A^T$.
(b) $T_2(A) = \det(A)$.

Solution:

(a)

$$(i)T_1(A+B) = (A+B)^T = A^T + B^T = T_1(A)+T_1(B).$$
$$(ii)T_1(kA) = (kA)^T = kA^T = kT_1(A),$$

so T_1 is linear.

(b) T_2 is not linear for

$$T_2(A+B) = \det(A+B) \neq \det(A)+\det(B) = T_2(A)+T_2(B).$$

■

1.1 Finding linear transformations from images of basis vectors

In this section, we show how to find the linear transformations from images of basis vectors.

If $T_A : R^n \to R^m$ is multiplication by A, and if $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n$ are the standard basis vectors for R^n, then A can be expressed as

$$A = [T(\mathbf{e}_1) | T(\mathbf{e}_2) | \cdots | T(\mathbf{e}_n)]$$

and we say A is *a matrix transformation*.
It follows from this that the image of any vector $\mathbf{v} = (c_1, c_2, \ldots, c_n)$ in R^n under multiplication by A can be expressed as

$$T_A(\mathbf{v}) = c_1 T_A(\mathbf{e}_1) + c_2 T_A(\mathbf{e}_2) + \cdots + c_n T_A(\mathbf{e}_n)$$

This formula tells us that for a matrix transformation the image of any vector is expressible as a linear combination of the images of the standard basis vectors. This is a special case of the following more general result.

Theorem 1.1.1 Let $T : V \to W$ be a linear transformation, where V is finite-dimensional. If $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a basis for V, then the image of any vector $\mathbf{v}$ in V can be expressed as

$$T(\mathbf{v}) = c_1 T(\mathbf{v}_1) + c_2 T(\mathbf{v}_2) + \cdots + c_n T(\mathbf{v}_n)$$

where $c_1, c_2, \ldots, c_n$ are the coefficients required to express $\mathbf{v}$ as a linear combination of the vectors in the basis S.

Proof. we write $\mathbf{v}$ as $\mathbf{v} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_n\mathbf{v}_n$ and use the linearity of T ■

■ **Example 1.7** Let $T : R^3 \to R^2$ be the linear transformation for which

$$T(\mathbf{v}_1) = (1,0), \quad T(\mathbf{v}_2) = (2,-1), \quad T(\mathbf{v}_3) = (4,3).$$

Find a formula for $T(x_1, x_2, x_3)$, and then use that formula to compute $T(2,-3,5)$ by using the basis $S = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ for R^3, where

$$\mathbf{v}_1 = (1,1,1), \quad \mathbf{v}_2 = (1,1,0), \quad \mathbf{v}_3 = (1,0,0).$$

Solution:
We first need to express $\mathbf{x} = (x_1, x_2, x_3)$ as a linear combination of $\mathbf{v}_1, \mathbf{v}_2$, and $\mathbf{v}_3$. If we write

$$(x_1, x_2, x_3) = c_1(1,1,1) + c_2(1,1,0) + c_3(1,0,0)$$

then on equating corresponding components, we obtain

$$\begin{aligned} c_1 + c_2 + c_3 &= x_1 \\ c_1 + c_2 \qquad &= x_2 \\ c_1 \qquad\quad &= x_3 \end{aligned}$$

which yields $c_1 = x_3, c_2 = x_2 - x_3, c_3 = x_1 - x_2$, so

$$\begin{aligned} (x_1, x_2, x_3) &= x_3(1,1,1) + (x_2 - x_3)(1,1,0) + (x_1 - x_2)(1,0,0) \\ &= x_3\mathbf{v}_1 + (x_2 - x_3)\mathbf{v}_2 + (x_1 - x_2)\mathbf{v}_3 \end{aligned}$$

Thus

$$\begin{aligned} T(x_1, x_2, x_3) &= x_3 T(\mathbf{v}_1) + (x_2 - x_3) T(\mathbf{v}_2) + (x_1 - x_2) T(\mathbf{v}_3) \\ &= x_3(1,0) + (x_2 - x_3)(2,-1) + (x_1 - x_2)(4,3) \\ &= (4x_1 - 2x_2 - x_3, 3x_1 - 4x_2 + x_3) \end{aligned}$$

From this formula we obtain

$$T(2,-3,5) = (9,2,3).$$

■

1.2 Kernel and range

In this section, we define and study the kernel and range of linear transformations.

Recall that if A is an $m \times n$ matrix, then the null space of A consists of all vectors x in R^n such that $Ax = 0$, and the column space of A consists of all vectors b in R^m for which there is at least one vector x in R^n such that $Ax = b$. From the viewpoint of matrix transformations, the null space of A consists of all vectors in R^n that multiplication by A maps into 0, and the column space of A consists of all vectors in R^m that are images of at least one vector in R^n under multiplication by A. The following definition extends these ideas to general linear transformations.

Definition 1.2.1 If $T : V \to W$ is a linear transformation, then the set of vectors in V that T maps into $\mathbf{0}$ is called the kernel of T and is denoted by $\ker(T)$. The set of all vectors in W that are images under T of at least one vector in V is called the range of T and is denoted by $R(T)$

■ **Example 1.8** Let $T : V \to W$ be the zero transformation. Find $Ker(T)$ and $R(T)$.

Solution:

Since T maps every vector in V into $\mathbf{0}$, it follows that $\ker(T) = V$. Moreover, since $\mathbf{0}$ is the only image under T of vectors in V, it follows that $R(T) = \{\mathbf{0}\}$.

■

■ **Example 1.9** Let $I : V \to V$ be the identity operator. Find $Ker(T)$ and $R(T)$.

Solution:

Since $I(\mathbf{v}) = \mathbf{v}$ for all vectors in V, every vector in V is the image of some vector (namely, itself); thus $R(I) = V$. Since the only vector that I maps into $\mathbf{0}$ is $\mathbf{0}$, it follows that $\ker(I) = \{\mathbf{0}\}$. ■

1.2.1 Properties of kernel and range

Theorem 1.2.1 If $T : V \to W$ is a linear transformation, then:

(a) The kernel of T is a subspace of V.

(b) The range of T is a subspace of W.

Proof. (a) To show that $\ker(T)$ is a subspace, we must show that it contains at least one vector and is closed under addition and scalar multiplication. Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be vectors in $\ker(T)$, and let k be any scalar. Then

$$T(\mathbf{v}_1+\mathbf{v}_2) = T(\mathbf{v}_1)+T(\mathbf{v}_2) = \mathbf{0}+\mathbf{0} = \mathbf{0}$$

so $\mathbf{v}_1+\mathbf{v}_2$ is in $\ker(T)$. Also,

$$T(k\mathbf{v}_1) = kT(\mathbf{v}_1) = k\mathbf{0} = \mathbf{0}$$

so $k\mathbf{v}_1$ is in $\ker(T)$.

(b) To show that $R(T)$ is a subspace of W, we must show that it contains at least one vector and is closed under addition and scalar multiplication. However, it contains at least the zero vector of W since $T(\mathbf{0}) = (\mathbf{0})$. To prove that it is closed under addition and scalar multiplication, we must show that if $\mathbf{w}_1$ and $\mid \mathbf{w}_2$ are vectors in $R(T)$, and if k is any scalar, then there exist vectors a and $\mathbf{b}$ in V for which

$$T(\mathbf{a}) = \mathbf{w}_1+\mathbf{w}_2 \quad \text{and} \quad T(\mathbf{b}) = k\mathbf{w}_1$$

But the fact that $\mathbf{w}_1$ and $\mathbf{w}_2$ are in $R(T)$ tells us there exist vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ in V such that

$$T(\mathbf{v}_1) = \mathbf{w}_1 \quad \text{and} \quad T(\mathbf{v}_2) = \mathbf{w}_2$$

The following computations complete the proof by showing that the vectors $\mathbf{a} = \mathbf{v}_1+\mathbf{v}_2$ and $\mathbf{b} = k\mathbf{v}_1$ satisfy the equations in (4):

$$\begin{aligned} T(\mathbf{a}) &= T(\mathbf{v}_1+\mathbf{v}_2) = T(\mathbf{v}_1)+T(\mathbf{v}_2) = \mathbf{w}_1+\mathbf{w}_2 \\ T(\mathbf{b}) &= T(k\mathbf{v}_1) = kT(\mathbf{v}_1) = k\mathbf{w}_1 \end{aligned}$$

■

1.3 Rank and nullity of linear transformations

In this section, we defined the notions of rank and nullity for an $m \times n$ matrix. Also, we proved that the sum of the rank and nullity is n.

Definition 1.3.1 Let $T : V \to W$ be a linear transformation. If the range of T is finite dimensional, then its dimension is called the rank of T; and if the kernel of T is finite-dimensional, then its dimension is called the nullity of T. The rank of T is denoted by rank (T) and the nullity of T by nullity (T).

Theorem 1.3.1 If $T : V \to W$ is a linear transformation from a finite-dimensional vector space V to a vector space W, then the range of T is finite-dimensional, and

$$\text{rank}(T) + \text{nullity}(T) = \dim(V).$$

Proof. Assume that V is n -dimensional. We must show that

$$\dim(R(T)) + \dim(\ker(T)) = n$$

We will give the proof for the case where $1 \leq \dim(\ker(T)) < n$. The cases where $\dim(\ker(T)) = 0$ and $\dim(\ker(T)) = n$ are left as exercises. Assume $\dim(\ker(T)) = r$ and let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be a basis for the kernel. Since $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ is linearly independent, Theorem 4.5.5(b) states that there are $n-r$ vectors, $\mathbf{v}_{r+1}, \ldots, \mathbf{v}_n$, such that the extended set $\{\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$ is a basis for V. To complete the proof, we will show that the $n-r$ vectors in the set $S = \{T(\mathbf{v}_{r+1}), \ldots, T(\mathbf{v}_n)\}$ form a basis for the range of T. It will then follow that

$$\dim(R(T)) + \dim(\ker(T)) = (n-r) + r = n$$

First we show that S spans the range of T. If $\mathbf{b}$ is any vector in the range of T, then $\mathbf{b} = T(\mathbf{v})$ for some vector $\mathbf{v}$ in V. Since $\{\mathbf{v}_1, \ldots, \mathbf{v}_r, \mathbf{v}_{r+1}, \ldots, \mathbf{v}_n\}$ is a basis for V, the vector v can be written in the form

$$\mathbf{v} = c_1\mathbf{v}_1 + \cdots + c_r\mathbf{v}_r + c_{r+1}\mathbf{v}_{r+1} + \cdots + c_n\mathbf{v}_n$$

Since $\mathbf{v}_1, \ldots, \mathbf{v}_r$ lie in the kernel of T, we have $T(\mathbf{v}_1) = \cdots = T(\mathbf{v}_r) = \mathbf{0}$, so

$$\mathbf{b} = T(\mathbf{v}) = c_{r+1}T(\mathbf{v}_{r+1}) + \cdots + c_nT(\mathbf{v}_n)$$

Thus S spans the range of T. Finally, we show that S is a linearly independent set and consequently forms a basis for the range of T. Suppose that some linear combination of the vectors in S is zero; that is,

$$k_{r+1}T(v_{r+1}) + \cdots + k_nT(\mathbf{v}_n) = 0 \tag{1.1}$$

We must show that $k_{r+1} = \cdots = k_n = 0$. Since T is linear, (3.5) can be rewritten as

$$T(k_{r+1}\mathbf{v}_{r+1} + \cdots + k_n\mathbf{v}_n) = \mathbf{0}$$

which says that $k_{r+1}\mathbf{v}_{r+1} + \cdots + k_n\mathbf{v}_n$ is in the kernel of T. This vector can therefore be written as a linear combination of the basis vectors $\{v_1, \ldots, v_r\}$, say

$$k_{r+1}\mathbf{v}_{r+1} + \cdots + k_n\mathbf{v}_n = k_1\mathbf{v}_1 + \cdots + k_r\mathbf{v}_r$$

Thus,

$$k_1\mathbf{v}_1 + \cdots + k_r\mathbf{v}_r - k_{r+1}\mathbf{v}_{r+1} - \cdots - k_n\mathbf{v}_n = \mathbf{0}$$

Since $\{v_1, \ldots, v_n\}$ is linearly independent, all of the k 's are zero; in particular, $k_{r+1} = \cdots = k_n = 0$, which completes the proof. ■

R In the special case where A is an $m \times n$ matrix and $T_A : R^n \to R^m$ is multiplication by A, the kernel of T_A is the null space of A, and the range of T_A is the column space o A. Thus, it follows from Theorem 1.3.1 that

$$\text{rank}(T_A) + \text{nullity}(T_A) = n$$

.

1.4 Composition linear transformations

In this section, we define one to one and onto linear transformations. Also, we discussed composition linear transformations.

Definition 1.4.1 If $T : V \to W$ is a linear transformation from a vector space V to a vector space W, then T is said to be one-to-one if T maps distinct vectors in V into distinct vectors in W, i.e.,

$$\forall u, v \in V, T(u) = T(v) \Rightarrow u = v.$$

Definition 1.4.2 If $T : V \to W$ is a linear transformation from a vector space V to a vector space W, then T is said to be onto (or onto W) if every vector in W is the image of at least one vector in V.

■ **Example 1.10** Let $T : R^2 \to R^2$ be a linear transformation define as

$$T(x,y) = (x, x+y).$$

(1) Find Ker T?
(2) Is T one-one?
(3) Is T onto?
Solution:
(1) Let $u = (x,y) \in KerT$, then

$$\begin{aligned} T(u) = O &\Rightarrow (x, x+y) = (0,0) \\ &\Rightarrow x = 0, x+y = 0 \\ &\Rightarrow x = y = 0, \end{aligned}$$

thus, $KerT = \{(0,0)\}$.
(2) Let $u = (x,y), v = (s,t) \in R^2$ and

$$\begin{aligned} T(u) = T(v) &\Rightarrow (x, x+y) = (s, s+t) \\ &\Rightarrow x = s, x+y = s+t \\ &\Rightarrow x = s, y = t \\ &\Rightarrow (x,y) = (s,t). \end{aligned}$$

thus, T is one-one.
(3) Let $v=(s,t)\in R^2$ and $v=T(u)$ for all $u=(x,y)\in R^2$, then

$$\begin{aligned} v=T(u) &\Rightarrow (s,t)=T(x,y)\\ &\Rightarrow (s,t)=(x,x+y)\\ &\Rightarrow x=s, y=t-s\\ &\Rightarrow (x,y)\in R^2. \end{aligned}$$

thus, T is onto. ∎

■ **Example 1.11** Let $T:R^2\to R^3$ be a linear transformation define as

$$T(x,y)=(x,x+y,x-y).$$

(1) Find Ker T?
(2) Is T one-one?
(3) Is T onto?
Solution:
(1) Let $u=(x,y)\in KerT$, then

$$\begin{aligned} T(u)=O &\Rightarrow (x,x+y,x-y)=(0,0,0)\\ &\Rightarrow x=0, x+y=0, x-y=0\\ &\Rightarrow x=y=0, \end{aligned}$$

thus, $KerT=\{(0,0)\}$.
(2) Let $u=(x,y), v=(s,t)\in R^2$ and

$$\begin{aligned} T(u)=T(v) &\Rightarrow (x,x+y,x-y)=(s,s+t,s-t)\\ &\Rightarrow x=s, x+y=s+t, x-y=s-t\\ &\Rightarrow x=s, y=t\\ &\Rightarrow (x,y)=(s,t)\\ &\Rightarrow u=v. \end{aligned}$$

thus, T is one-one.

(3) Let $v=(s,t,e)\in R^3$ and $v=T(u)$ for all $u=(x,y)\in R^2$, then

$$\begin{aligned} v=T(u) &\Rightarrow (s,t,e)=T(x,y)\\ &\Rightarrow (s,t,e)=(x,x+y,x-y)\\ &\Rightarrow x=s, y=t-s, y=s-e, \end{aligned}$$

i.e., y has two values. Thus, T is not onto. ∎

Theorem 1.4.1 If $T:V\to W$ is a linear transformation, then the following statements are equivalent.
(a) T is one-to-one.
(b) $\ker(T)=\{\mathbf{0}\}$.

Proof. $(a)\Rightarrow(b)$ Since T is linear, we know that $T(\mathbf{0})=\mathbf{0}$. Since T is one-to-one, there can be no other vectors in V that map into $\mathbf{0}$, so $\ker(T)=\{\mathbf{0}\}$. $(b)\Rightarrow(a)$ Assume that $\ker(T)=\{0\}$. If $\mathbf{u}$ and $\mathbf{v}$ are distinct vectors in V, then $\mathbf{u}-\mathbf{v}\neq\mathbf{0}$. This implies that $T(\mathbf{u}-\mathbf{v})\neq\mathbf{0}$, for otherwise $\ker(T)$ would contain a nonzero vector. Since T is linear, it follows that

$$T(\mathbf{u})-T(\mathbf{v})=T(\mathbf{u}-\mathbf{v})\neq\mathbf{0}$$

so T maps distinct vectors in V into distinct vectors in W and hence is one-to-one. ■

Definition 1.4.3 If $T_1:U\to V$ and $T_2:V\to W$ are linear transformations, then the composition of T_2 with T_1, denoted by $T_2\circ T_1$ (which is read " T_2 circle T_1"), is the function defined by the formula

$$(T_2\circ T_1)(\mathbf{u})=T_2(T_1(\mathbf{u}))$$

where $\mathbf{u}$ is a vector in U.

Theorem 1.4.2 Let $T_1:U\to V$ and $T_2:V\to W$ be a linear transformations, then $(T_2\circ T_1):U\to W$ is also a linear transformation.

Proof. Suppose that $\mathbf{u}$ and $\mathbf{v}$ are vectors in U and c is a scalar, then it follows from (1) and the linearity of T_1 and T_2 that

$$\begin{aligned}(T_2 \circ T_1)(\mathbf{u}+\mathbf{v}) &= T_2(T_1(\mathbf{u}+\mathbf{v})) = T_2(T_1(\mathbf{u})+T_1(\mathbf{v})) \\ &= T_2(T_1(\mathbf{u}))+T_2(T_1(\mathbf{v})) \\ &= (T_2 \circ T_1)(\mathbf{u})+(T_2 \circ T_1)(\mathbf{v})\end{aligned}$$

and

$$\begin{aligned}(T_2 \circ T_1)(c\mathbf{u}) &= T_2(T_1(c\mathbf{u})) = T_2(cT_1(\mathbf{u})) \\ &= cT_2(T_1(\mathbf{u})) = c(T_2 \circ T_1)(\mathbf{u})\end{aligned}$$

Thus, $T_2 \circ T_1$ satisfies the two requirements of a linear transformation. ■

■ **Example 1.12** Let $T_1 : P_1 \to P_2$ and $T_2 : P_2 \to P_2$ be the linear transformations given by the formulas

$$T_1(p(x)) = xp(x) \text{ and } T_2(p(x)) = p(2x+4)$$

Then find $(T_2 \circ T_1)$.
Solution:
The composition $(T_2 \circ T_1) : P_1 \to P_2$ is given by the formula

$$(T_2 \circ T_1)(p(x)) = T_2(T_1(p(x))) = T_2(xp(x)) = (2x+4)p(2x+4)$$

In particular, if $p(x) = c_0 + c_1 x$, then

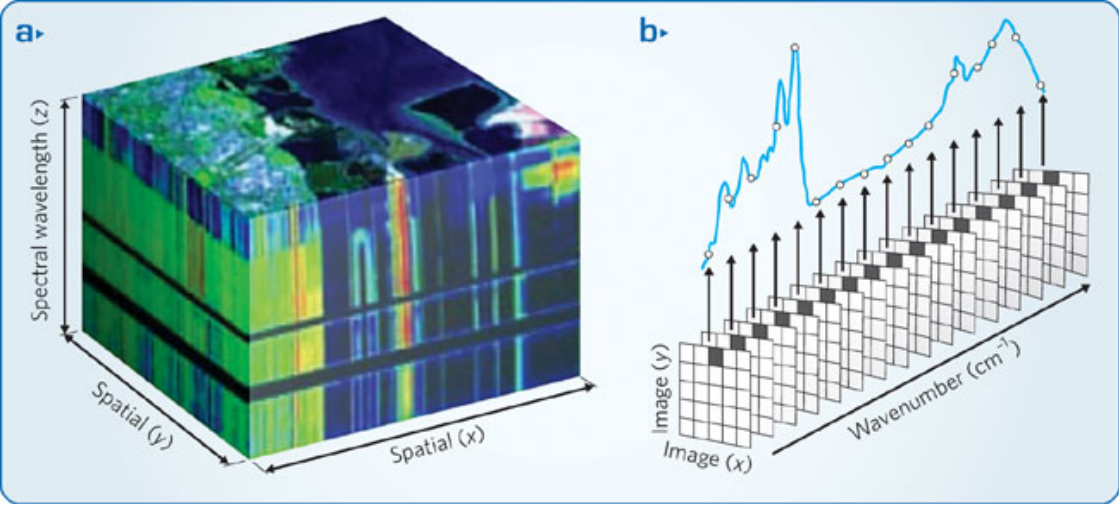
$$\begin{aligned}(T_2 \circ T_1)(p(x)) &= (T_2 \circ T_1)(c_0+c_1x) = (2x+4)(c_0+c_1(2x+4)) \\ &= c_0(2x+4)+c_1(2x+4)^2.\end{aligned}$$

■

1.5 Exercises

1. Suppose that T is a mapping whose domain is the vector space M_{22}. In each part, determine whether T is a linear transformation, and if so, find its kernel.
   (a) $T(A) = A^2$.
   (b) $T(A) = \text{tr}(A)$.
   (c) $T(A) = A + A^T$.
   (d) $T(A) = (A)_{11}$
   (e) $T(A) = 0_{2\times 2}$
   (f) $T(A) = cA$
2. Determine whether the mapping T is a linear transformation, and if so, find its kernel.
   (a) $T : R^3 \to R$, where $T(\mathbf{u}) = \|\mathbf{u}\|$.
   (b) $T : R^3 \to R^3$, where v_0 is a fixed vector in R^3 and $T(\mathbf{u}) = \mathbf{u} \times \mathbf{v}_0$.
   (c) $T : M_{22} \to M_{23}$, where B is a fixed 2×3 matrix and $T(A) = AB$.
   (d) $T : M_{22} \to R$, where
      (i) $T\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = 3a - 4b + c - d$
      (ii) $T\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a^2 + b^2$
   (e) $T : P_2 \to P_2$, where
      (i) $T\left(a_0 + a_1x + a_2x^2\right) = a_0 + a_1(x+1) + a_2(x+1)^2$
      (ii) $T\left(a_0 + a_1x + a_2x^2\right) = (a_0 + 1) + (a_1 + 1)x + (a_2 + 1)x^2$
   (f) $T : F(-\infty, \infty) \to F(-\infty, \infty)$, where (a) $T(f(x)) = 1 + f(x)$ (b) $T(f(x)) = f(x+1)$
3. Let $T : P_2 \to P_3$ be the linear transformation defined by $T(p(x)) = xp(x)$. Which of the following are in $\ker(T)$?
   (a) x^2
   (b) 0
   (c) $1 + x$
   (d) $-x$
4. Let $T : M_{22} \to M_{22}$ be the dilation operator with factor $k = 3$.
   (a) Find $T\left(\begin{bmatrix} 1 & 2 \\ -4 & 3 \end{bmatrix}\right)$.
   (b) Find the rank and nullity of T.

5. Let $T : P_2 \to P_2$ be the contraction operator with factor $k = 1/4$
   (a) Find $T\left(1+4x+8x^2\right)$.
   (b) Find the rank and nullity of T.
6. Determine whether the linear transformation is one-to-one and onto by finding its kernel:
   (a) $T : R^2 \to R^2$, where $T(x,y) = (y,x)$.
   (b) $T : R^2 \to R^3$, where $T(x,y) = (x,y,x+y)$.
   (c) $T : R^3 \to R^2$, where $T(x,y,z) = (x+y+z, x-y-z)$.
   (d) $T : R^2 \to R^3$, where $T(x,y) = (x-y, y-x, 2x-2y)$.
   (e) $T : R^2 \to R^2$, where $T(x,y) = (0, 2x+3y)$.
   (f) $T : R^2 \to R^2$, where $T(x,y) = (x+y, x-y)$.



2. Eigenvalues and Eigenve

In this chapter, we'll look at the "eigenvalues" and "eigenvectors" of scalars and vectors, words derived from the German word eigen, which means "own," "peculiar to," "characteristic," or "individual." The fundamental definition was first used in the study of rotational motion, but it was later applied to distinguish various types of surfaces and to explain solutions to differential equations.

Definition 2.0.1 If A is an $n \times n$ matrix, then a nonzero vector $\mathbf{x}$ in R^n is called an eigenvector of A (or of the matrix operator T_A) if $A\mathbf{x}$ is a scalar multiple of $\mathbf{x}$; that is,

$$A\mathbf{x} = \lambda\mathbf{x}$$

for some scalar λ. The scalar λ is called an **eigenvalue** of A (or of T_A), and $\mathbf{x}$ is said to be an **eigenvector** corresponding to λ.

Computing Eigenvalues and Eigenvectors

Our next goal is to establish a general method for determining the eigenvalues and eigenvectors of an $n \times n$ matrix A. We will begin with the problem of finding the eigenvalues of A. Note first that the equation $A\mathbf{x} = \lambda\mathbf{x}$ can be rewritten as $A\mathbf{x} = \lambda I\mathbf{x}$, or equivalently, as

$$(\lambda I - A)\mathbf{x} = \mathbf{0}$$

For λ to be an eigenvalue of A this equation must have a nonzero solution for $\mathbf{x}$. The coefficient matrix $\lambda I - A$ has a zero determinant. Thus, we have the following result.

Theorem 2.0.1 If A is an $n \times n$ matrix, then λ is an eigenvalue of A if and only if it satisfies the equation

$$\det(\lambda I - A) = 0 \tag{2.1}$$

This is called the characteristic equation of A.

■ **Example 2.1** Finding eigenvalues of the matrix

$$A = \begin{bmatrix} 3 & 0 \\ 8 & -1 \end{bmatrix}.$$

Solution:
The eigenvalues of A are the solutions of the equation

$$\det(\lambda I - A) = 0,$$

which we can write as

$$\begin{vmatrix} \lambda - 3 & 0 \\ -8 & \lambda + 1 \end{vmatrix} = 0,$$

from which we obtain

$$(\lambda - 3)(\lambda + 1) = 0.$$

Thus, the eigenvalues of A are $\lambda = 3$ and $\lambda = -1$. ■

When the determinant $\det(\lambda I - A)$ in (2.1) is expanded, the characteristic equation of A takes the form

$$\lambda^n + c_1\lambda^{n-1} + \cdots + c_n = 0 \tag{2.2}$$

where the left side of this equation is a polynomial of degree n in which the coefficient of λ^n is 1. The polynomial

$$p(\lambda) = \lambda^n + c_1\lambda^{n-1} + \cdots + c_n \tag{2.3}$$

is called the **characteristic polynomial** of A.

■ **Example 2.2** Recall Example (4.3), the characteristic polynomial of the 2×2 matrix is

$$p(\lambda) = (\lambda - 3)(\lambda + 1) = \lambda^2 - 2\lambda - 3$$

which is a polynomial of degree 2 . ■

Since a polynomial of degree n has at most n distinct roots, it follows from (2.2) that the characteristic equation of an $n \times n$ matrix A has at most n distinct solutions and consequently the matrix has at most n distinct eigenvalues. Since some of these solutions may be complex numbers, it is possible for a matrix to have complex eigenvalues, even if that matrix itself has real entries.

■ **Example 2.3** Find the eigenvalues of

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 4 & -17 & 8 \end{bmatrix}$$

Solution:
The characteristic polynomial of A is

$$\det(\lambda I - A) = \det \begin{bmatrix} \lambda & -1 & 0 \\ 0 & \lambda & -1 \\ -4 & 17 & \lambda - 8 \end{bmatrix} = \lambda^3 - 8\lambda^2 + 17\lambda - 4$$

The eigenvalues of A must therefore satisfy the cubic equation

$$\lambda^3 - 8\lambda^2 + 17\lambda - 4 = 0,$$

and we can be rewritten the above equation as

$$(\lambda - 4)(\lambda^2 - 4\lambda + 1) = 0,$$

Thus, the eigenvalues of A are

$$\lambda = 4, \lambda = 2 + \sqrt{3}, \textit{ and } \lambda = 2 - \sqrt{3}.$$

■

■ **Example 2.4** Find the eigenvalues of the upper triangular matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & 0 & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{bmatrix}.$$

Solution:
The determinant of a triangular matrix is the product of the entries on the main diagonal, we obtain

$$\begin{aligned} \det(\lambda I - A) &= \det \begin{bmatrix} \lambda - a_{11} & -a_{12} & -a_{13} & -a_{14} \\ 0 & \lambda - a_{22} & -a_{23} & -a_{24} \\ 0 & 0 & \lambda - a_{33} & -a_{34} \\ 0 & 0 & 0 & \lambda - a_{44} \end{bmatrix} \\ &= (\lambda - a_{11})(\lambda - a_{22})(\lambda - a_{33})(\lambda - a_{44}) \end{aligned}$$

Thus, the characteristic equation is

$$(\lambda - a_{11})(\lambda - a_{22})(\lambda - a_{33})(\lambda - a_{44}) = 0$$

and the eigenvalues are

$$\lambda = a_{11}, \quad \lambda = a_{22}, \quad \lambda = a_{33}, \quad \lambda = a_{44}$$

which are precisely the diagonal entries of A. ■

Theorem 2.0.2 If A is an $n \times n$ triangular matrix (upper triangular, lower triangular, or diagonal), then the eigenvalues of A are the entries on the main diagonal of A

Theorem 2.0.3 If A is an $n \times n$ matrix, the following statements are equivalent.
(a) λ is an eigenvalue of A.
(b) λ is a solution of the characteristic equation $\det(\lambda I - A) = 0$.
(c) The system of equations $(\lambda I - A)\mathbf{x} = \mathbf{0}$ has nontrivial solutions.
(d) There is a nonzero vector $\mathbf{x}$ such that $A\mathbf{x} = \lambda\mathbf{x}$.

Finding Eigenvectors and Bases for Eigenspaces:
Now that we know how to find the eigenvalues of a matrix, we will consider the problem of finding the corresponding eigenvectors. By definition, the eigenvectors of A corresponding to an eigenvalue λ are the nonzero vectors that satisfy

$$(\lambda I - A)x = O.$$

Thus, we can find the eigenvectors of A corresponding to λ by finding the nonzero vector x which it is a solution of the system $(\lambda I - A)x = O$.

■ **Example 2.5** Find bases for the eigenvectors of the matrix

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

Solution:
The characteristic equation of A is

$$\begin{vmatrix} \lambda + 1 & -3 \\ -2 & \lambda \end{vmatrix} = \lambda(\lambda + 1) - 6 = (\lambda - 2)(\lambda + 3) = 0$$

so the eigenvalues of A are $\lambda = 2$ and $\lambda = -3$.
Thus, there are two eigenvectors of A, one for each eigenvalue. By definition, suppose that

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

is an eigenvector of A corresponding to an eigenvalue λ if and only if $(\lambda I - A)\mathbf{x} = 0$, that is,

$$\begin{bmatrix} \lambda+1 & -3 \\ -2 & \lambda \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

In the case where $\lambda = 2$ this equation becomes

$$\begin{bmatrix} 3 & -3 \\ -2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

whose general solution is

$$x_1 = t, \quad x_2 = t.$$

Since this can be written in matrix form as

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} t \\ t \end{bmatrix} = t \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

it follows that

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

is a basis for the eigenvectors corresponding to $\lambda = 2$. We leave it for you to follow the pattern of these computations and show that

$$\begin{bmatrix} -\frac{3}{2} \\ 1 \end{bmatrix}$$

is a basis for the eigenspace corresponding to $\lambda = -3$. ■

■ **Example 2.6** Find bases for the eigenvectors of

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

Solution:
The characteristic equation of A is

$$\lambda^3 - 5\lambda^2 + 8\lambda - 4 = 0,$$

or in factored form,

$$(\lambda - 1)(\lambda - 2)^2 = 0.$$

Thus, the distinct eigenvalues of A are $\lambda = 1$ and $\lambda = 2$, so there are two eigenvectors of A. By definition,

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

is an eigenvector of A corresponding to λ if and only if $\mathbf{x}$ is a nontrivial solution of $(\lambda I - A)\mathbf{x} = 0$, or in matrix form,

$$\begin{bmatrix} \lambda & 0 & 2 \\ -1 & \lambda - 2 & -1 \\ -1 & 0 & \lambda - 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

In the case where $\lambda = 2$, the above equation becomes

$$\begin{bmatrix} 2 & 0 & 2 \\ -1 & 0 & -1 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Solving this system using Gaussian elimination yields

$$x_1 = -s, \quad x_2 = t, \quad x_3 = s$$

Thus, the eigenvectors of A corresponding to $\lambda = 2$ are the nonzero vectors of the form

$$\mathbf{x} = \begin{bmatrix} -s \\ t \\ s \end{bmatrix} = \begin{bmatrix} -s \\ 0 \\ s \end{bmatrix} + \begin{bmatrix} 0 \\ t \\ 0 \end{bmatrix} = s \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} + t \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Sin

$$\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

are linearly independent (why?), these vectors form a basis for the eigenvector corresponding to $\lambda = 2$.
If $\lambda = 1$, then $(\lambda I - A)x = O$ becomes

$$\begin{bmatrix} 1 & 0 & 2 \\ -1 & -1 & -1 \\ -1 & 0 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Solving this system yields (verify)

$$x_1 = -2s, \quad x_2 = s, \quad x_3 = s$$

Thus, the eigenvectors corresponding to $\lambda = 1$ are the nonzero vectors of the form

$$\begin{bmatrix} -2s \\ s \\ s \end{bmatrix} = s \begin{bmatrix} -2 \\ 1 \\ 1 \end{bmatrix} \text{ so that } \begin{bmatrix} -2 \\ 1 \\ 1 \end{bmatrix}$$

is a basis for the eigenspace corresponding to $\lambda = 1$. ∎

The next theorem establishes a relationship between the eigenvalues and the invertibility of a matrix.

Theorem 2.0.4 A square matrix A is invertible if and only if $\lambda = 0$ is not an eigenvalue of A.

Proof. Assume that A is an $n \times n$ matrix and observe first that $\lambda = 0$ is a solution of the characteristic equation

$$\lambda^n + c_1\lambda^{n-1} + \cdots + c_n = 0$$

if and only if the constant term c_n is zero. Thus, it suffices to prove that A is invertible if and only if $c_n \neq 0$. But

$$\det(\lambda I - A) = \lambda^n + c_1\lambda^{n-1} + \cdots + c_n$$

or, on setting $\lambda = 0$,

$$\det(-A) = c_n \quad \text{or} \quad (-1)^n \det(A) = c_n$$

It follows from the last equation that $\det(A) = 0$ if and only if $c_n = 0$, and this in turn implies that A is invertible if and only if $c_n \neq 0$. ■

2.1 Exercises

A- Find eigenvalue and eigenvectors of the following:

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

B- Find the characteristic equation, the eigenvalues, and bases for the eigenvectors of the matrix.

(a) $\begin{bmatrix} 1 & 4 \\ 2 & 3 \end{bmatrix}$.

(b) $\begin{bmatrix} -2 & -7 \\ 1 & 2 \end{bmatrix}$.

(c) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

(d) $\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$.

(e) $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$.

(f) $\begin{bmatrix} 2 & -3 \\ 0 & 2 \end{bmatrix}$.

(i) $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$.

(u) $\begin{bmatrix} 1 & 2 \\ -2 & -1 \end{bmatrix}$.

C- Find the characteristic equation, the eigenvalues, and bases for the eigenvectors of the matrix.

1. $\begin{bmatrix} 4 & 0 & 1 \\ -2 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix}$.
2. $\begin{bmatrix} 1 & 0 & -2 \\ 0 & 0 & 0 \\ -2 & 0 & 4 \end{bmatrix}$.
3. $\begin{bmatrix} 6 & 3 & -8 \\ 0 & -2 & 0 \\ 1 & 0 & -3 \end{bmatrix}$.
4. $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.
5. $\begin{bmatrix} 4 & 0 & -1 \\ 0 & 3 & 0 \\ 1 & 0 & 2 \end{bmatrix}$.
6. $\begin{bmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{bmatrix}$.

2.2 Diagonalization

Definition 2.2.1 If A and B are square matrices, then we say that B is similar to A if there is an invertible matrix P such that

$$B = P^{-1}AP.$$

Note that if B is similar to A, then it is also true that A is similar to B since we can express A as $A = Q^{-1}BQ$ by taking $Q = P^{-1}$. This being the case, we will usually say that A and B are similar matrices if either is similar to the other.

Definition 2.2.2 A square matrix A is said to be diagonalizable if it is similar to some diagonal matrix; that is, if there exists an invertible matrix P such that $P^{-1}AP$ is diagonal. In this case the matrix P is said to diagonalize A.

Theorem 2.2.1 (a) If $\lambda_1, \lambda_2, \ldots, \lambda_k$ are distinct eigenvalues of a matrix A, and if $v_1, v_2, \ldots, v_k$ are corresponding eigenvectors, then $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is a linearly independent set.
(b) An $n \times n$ matrix with n distinct eigenvalues is diagonalizable.

A Procedure for Diagonalizing an $n \times n$ Matrix

Step 1 . Determine first whether the matrix is actually diagonalizable by searching for n linearly independent eigenvectors. One way to do this is to find a basis for each eigenvector and count the total number of vectors obtained. If there is a total of n vectors, then the matrix is diagonalizable, and if the total is less than n, then it is not.
Step 2. If you ascertained that the matrix is diagonalizable, then form the matrix $P = [\mathbf{p}_1\ \mathbf{p}_2 \ldots \mathbf{p}_n]$ whose column vectors are the n basis vectors you obtained in Step 1.
Step 3. P^{-1} AP will be a diagonal matrix whose successive diagonal entries are the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ that correspond to the successive columns of P.

■ **Example 2.7** Find a matrix P that diagonalizes

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

Solution:
The characteristic equation of A to be

$$(\lambda - 1)(\lambda - 2)^2 = 0$$

and we found the following bases for the eigenvalues:

$$\lambda = 2: \quad p_1 = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}: \quad \lambda = 1: \quad p_3 = \begin{bmatrix} -2 \\ 1 \\ 1 \end{bmatrix}$$

There are three basis vectors in total, so the matrix

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

diagonalizes A. As a check, you should verify that

$$P^{-1}AP = \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix} \begin{bmatrix} -1 & 0 & -2 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

In general, there is no preferred order for the columns of P. Since the i th diagonal entry of $P^{-1}AP$ is an eigenvalue for the i th column vector of P, changing the order of the columns of P just changes the order of the eigenvalues on the diagonal of $P^{-1}AP$. Thus, had we written

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

in the preceding example, we would have obtained

$$P^{-1}AP = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

■

■ **Example 2.8** Show that the following matrix is not diagonalizable:

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

Solution:
The characteristic polynomial of A is

$$\det(\lambda I - A) = \begin{vmatrix} \lambda - 1 & 0 & 0 \\ -1 & \lambda - 2 & 0 \\ 3 & -5 & \lambda - 2 \end{vmatrix} = (\lambda - 1)(\lambda - 2)^2$$

so the characteristic equation is

$$(\lambda - 1)(\lambda - 2)^2 = 0$$

and the distinct eigenvalues of A are $\lambda = 1$ and $\lambda = 2$. We leave it for you to show that bases for the eigenvalues are

$$\lambda = 1: \quad \mathbf{p}_1 = \begin{bmatrix} \frac{1}{8} \\ -\frac{1}{8} \\ 1 \end{bmatrix}; \quad \lambda = 2: \quad \mathbf{p}_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Since A is a 3×3 matrix and there are only two basis vectors in total A is not diagonalizable. ■

2.2.1 Eigenvalues of Powers of a Matrix

Suppose that λ is an eigenvalue of A and $\mathbf{x}$ is a corresponding eigenvector. Then

$$A^2\mathbf{x} = A(A\mathbf{x}) = A(\lambda\mathbf{x}) = \lambda(A\mathbf{x}) = \lambda(\lambda\mathbf{x}) = \lambda^2\mathbf{x}$$

which shows not only that λ^2 is a eigenvalue of A^2 but that $\mathbf{x}$ is a corresponding eigenvector. In general, we have the following result.

Theorem 2.2.2 If k is a positive integer, λ is an eigenvalue of a matrix A, and $\mathbf{x}$ is a corresponding eigenvector, then λ^k is an eigenvalue of A^k and $\mathbf{x}$ is a corresponding eigenvector.

■ **Example 2.9** In Example 2.8 we found the eigenvalues and corresponding eigenvectors of the matrix

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

Do the same for A^7.

Solution:

We know from Example 2.8 that the eigenvalues of A are $\lambda = 1$ and $\lambda = 2$, so the eigenvalues of A^7 are $\lambda = 1^7 = 1$ and $\lambda = 2^7 = 128$. The eigenvectors $\mathbf{p}_1$ and $\mathbf{p}_2$ obtained in Example 2.8 corresponding to the eigenvalues $\lambda = 1$ and $\lambda = 2$ of A are also the eigenvectors corresponding to the eigenvalues $\lambda = 1$ and $\lambda = 128$ of A^7. ■

Computing Powers of a Matrix;

Suppose that A is a diagonalizable $n \times n$ matrix, that P diagonalizes A, and that

$$P^{-1}AP = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} = D$$

Squaring both sides of this equation yields

$$\left(P^{-1}AP\right)^2 = \begin{bmatrix} \lambda_1^2 & 0 & \cdots & 0 \\ 0 & \lambda_2^2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n^2 \end{bmatrix} = D^2$$

We can rewrite the left side of this equation as

$$\left(P^{-1}AP\right)^2 = P^{-1}APP^{-1}AP = P^{-1}AIAP = P^{-1}A^2P$$

from which we obtain the relationship $P^{-1}A^2P = D^2$. More generally, if k is a positive integer, then a similar computation will show that

$$P^{-1}A^kP = D^k = \begin{bmatrix} \lambda_1^k & 0 & \cdots & 0 \\ 0 & \lambda_2^k & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n^k \end{bmatrix}$$

which we can rewrite as

$$A^k = PD^kP^{-1} = P \begin{bmatrix} \lambda_1^k & 0 & \cdots & 0 \\ 0 & \lambda_2^k & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n^k \end{bmatrix} P^{-1}.$$

■ **Example 2.10** Find A^{13}, where

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

Solution:
Recall Example 2.7 that the matrix A is diagonalized by

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

and that

$$D = P^{-1}AP = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus, it follows that

$$A^{13} = PD^{13}P^{-1} = \begin{bmatrix} -1 & 0 & -2 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2^{13} & 0 & 0 \\ 0 & 2^{13} & 0 \\ 0 & 0 & 1^{13} \end{bmatrix} \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ -1 & 0 & -1 \end{bmatrix}$$
$$= \begin{bmatrix} -8190 & 0 & -16382 \\ 8191 & 8192 & 8191 \\ 8191 & 0 & 16383 \end{bmatrix}.$$

■

2.3 Exercise

A- Show that A and B are not similar matrices

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

2. $A = \begin{bmatrix} 4 & -1 \\ 2 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 4 & 1 \\ 2 & 4 \end{bmatrix}$

3. $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 0 \\ \frac{1}{2} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

4. $A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 0 & 2 \\ 3 & 0 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 2 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ B- Find a matrix P that diagonalizes A, and check your work by computing $P^{-1}AP$.

5. $A = \begin{bmatrix} 1 & 0 \\ 6 & -1 \end{bmatrix}$

6. $A = \begin{bmatrix} -14 & 12 \\ -20 & 17 \end{bmatrix}$.

7. $A = \begin{bmatrix} 2 & 0 & -2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$. 8. $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

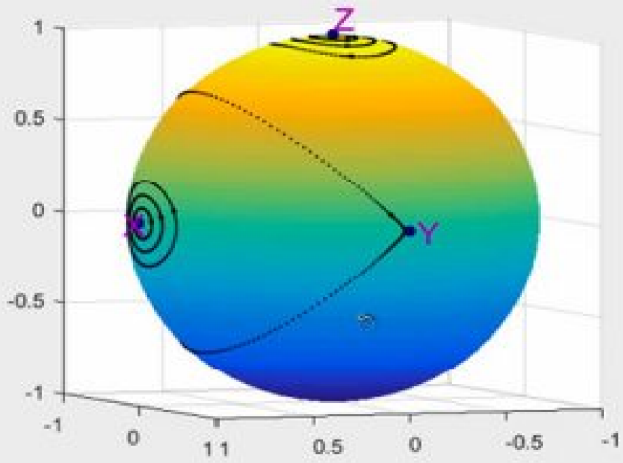
9. Let

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

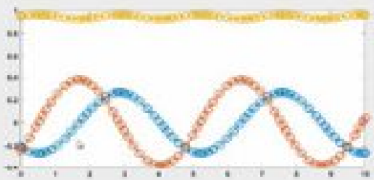
(a) Find the eigenvalues of A.
(b) For each eigenvalue λ, find the rank of the matrix $\lambda I - A$.
(c) Is A diagonalizable? Justify your conclusion.

Part II

Applications of Linear Algebra



$$\frac{d}{dt}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} yz \\ -2xz \\ xy \end{pmatrix}$$



3. Differential Equations

Many laws of physics, chemistry, biology, engineering, and economics are described in terms of "differential equations"—that is, equations involving functions and their derivatives. In this section we will illustrate one way in which matrix diagonalization can be used to solve systems of differential equations.

Recall from calculus that a differential equation is an equation involving unknown functions and their derivatives. The order of a differential equation is the order of the highest derivative it contains. The simplest differential equations are the first-order equations of the form

$$y' = ay \tag{3.1}$$

where $y = f(x)$ is an unknown differentiable function to be determined, $y' = dy/dx$ is its derivative, and a is a constant. As with most differential equations, this equation has infinitely many solutions; they are the functions

of the form

$$y = ce^{ax} \tag{3.2}$$

where c is an arbitrary constant. That every function of this form is a solution of 3.1 follows from the computation

$$y' = cae^{ax} = ay$$

and that these are the only solution is shown in the exercises. Accordingly, we call 3.2 the general solution of 3.1. As an example, the general solution of the differential equation $y' = 5y$ is

$$y = ce^{5x} \tag{3.3}$$

Often, a physical problem that leads to a differential equation imposes some conditions that enable us to isolate one particular solution from the general solution. For example, if we require that solution 3.3 of the equation $y' = 5y$ satisfy the added condition

$$y(0) = 6 \tag{3.4}$$

(that is, $y = 6$ when $x = 0$), then on substituting these values in 3.3, we obtain $6 = ce^0 = c$, from which we conclude that

$$y = 6e^{5x}$$

is the only solution $y' = 5y$ that satisfies 3.4.

A condition such as 3.4, which specifies the value of the general solution at a point, is called an **initial condition**, and the problem of solving a differential equation subject to an initial condition is called an **initial-value problem.**

3.1 First-Order Linear Systems

A systems of differential equations of the form

$$\begin{aligned} y_1' &= a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n \\ y_2' &= a_{21}y_1 + a_{22}y_2 + \cdots + a_{2n}y_n \\ &\vdots \\ y_n' &= a_{n1}y_1 + a_{n2}y_2 + \cdots + a_{nn}y_n \end{aligned} \tag{3.5}$$

where $y_1 = f_1(x), y_2 = f_2(x), \ldots, y_n = f_n(x)$ are functions to be determined, and the a_{ij} s are constants.

By using matrix notation, (3.5) can be written as

$$\begin{bmatrix} y_1' \\ y_2' \\ \vdots \\ y_n' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

or

$$y' = Ay \tag{3.6}$$

where the notation y' denotes the vector obtained by differentiating each component of y.

We call (3.5) or its matrix form (3.6) a constant coefficient first-order homogeneous linear system. It is of first order because all derivatives are of that order, it is linear because differentiation and matrix multiplication are linear transformations, and it is homogeneous because

$$y_1 = y_2 = \cdots = y_n = 0$$

is a solution regardless of the values of the coefficients As expected, this is called the trivial solution.

■ **Example 3.1** Write the following system in matrix form:

$$\begin{aligned} y_1' &= 3y_1 \\ y_2' &= -2y_2 \\ y_3' &= 5y_3 \end{aligned}$$

Solution:

$$\begin{bmatrix} y_1' \\ y_2' \\ y_3' \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

or

$$y' = \begin{bmatrix} 3 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 5 \end{bmatrix} \mathrm{y}$$

■

■ **Example 3.2** Solve the system in the above Example (3.1)
Solution:
Since the above system involves only one unknown function, we can solve the equations individually. then the solutions are

$$\begin{aligned} y_1 &= c_1 e^{\mathrm{t}x} \\ y_2 &= c_2 e^{-2x} \\ y_3 &= c_3 e^{\mathrm{s}x} \end{aligned}$$

or, in matrix notation,

$$y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} c_1 e^{\mathrm{s}x} \\ c_2 e^{-2} \\ c_{\mathrm{s}} e^{4x} \end{bmatrix}$$

■

■ **Example 3.3** Find a solution of the system in the above Example (3.1) that satisfies the initial conditions $y_1(0) = 1$, $y_2(0) = 4$, and $y_3(0) = -2$
Solution:
From the given initial conditions, we obtain

$$\begin{aligned} 1 = y_1(0) &= c_1 e^0 = c_1 \\ 4 = y_2(0) &= c_2 e^0 = c_2 \\ -2 = y_3(0) &= cse^0 = c_3 \end{aligned}$$

so the solution satisfying these conditions is

$$y_1 = e^{3x}, \quad y_2 = 4e^{-2x}, \quad y_3 = -2e^{4x}$$

or, in matrix notation,

$$\mathrm{y} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} e^{3x} \\ 4e^{-2x} \\ -2e^{4x} \end{bmatrix}.$$

■

3.2 Solve First-Order Linear System by Diagonalization

The basic idea for solving a system

$$y' = Ay$$

whose coefficient matrix A is not diagonal is to introduce a new unknown vector u that is related to the unknown vector y by an equation of the form

$$y = Pu$$

in which P is an invertible matrix that diagonalizes A. Of course, such a matrix may or may not exist, but if it does, then we can rewrite the equation

$$y' = Ay$$

as

$$P\mathrm{u}' = A(P\mathrm{u})$$

or alternatively as

$$\mathbf{u}' = \left(P^{-1}AP\right)\mathbf{u}$$

Since P is assumed to diagonalizes A, this equation has the form

$$\mathbf{u}' = D\mathbf{u}$$

where D is diagonal. We can now solve this equation for u using the method of Example (3.1), and then obtain y by matrix multiplication using the relationship $y = P\mathrm{u}$.

In summary, we have the following procedure for solving a system $y' = Ay$ in the case were A is diagonalizable.

A Procedure for Solving $y' = Ay$ If A Is Diaganalizable

Step 1. Find a matrix P that dizgonalizes A.
Step 2. Make the substitutions $\mathrm{y} = P\mathrm{u}$ and $y' = P\mathrm{u}'$ to obtain a new "diagonal system"

$$\mathrm{u}' = D\mathrm{u},$$

where $D = P^{-1}AP$.
Step 3. Solve $u' = D\mathbf{u}$.
Step 4. Determine y from the equation $\mathrm{y} = P\mathrm{u}$.

■ **Example 3.4** Let a system

$$\begin{aligned} y_1' &= y_1 + y_2 \\ y_2' &= 4y_1 - 2y_2 \end{aligned}$$

then
(a) Solve this system.
(b) Find the solution that satisfies the initial conditions $y_1(0) = 1, y_2(0) = 6$.
Solution:
(a) The coefficient matrix for the system is

$$A = \begin{bmatrix} 1 & 1 \\ 4 & -2 \end{bmatrix}.$$

Since A will be diagonalized by any matrix P whose columns are linearly independent eigenvectors of A.
Now

$$\begin{aligned} \det(\lambda I - A) &= \begin{vmatrix} \lambda - 1 & -1 \\ -4 & \lambda + 2 \end{vmatrix} \\ &= \lambda^2 + \lambda - 6 \\ &= (\lambda + 3)(\lambda - 2), \end{aligned}$$

the eigenvalues of A are $\lambda = 2$ and $\lambda = -3$.
By definition,

$$\mathrm{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

is an eigenvector of A corresponding to λ if and only if x is a nontrivial solution of

$$\begin{bmatrix} \lambda-1 & -1 \\ -4 & \lambda+2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

If $\lambda = 2$, this system becomes

$$\begin{bmatrix} 1 & -1 \\ -4 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Solving this system yields $x_1 = t, x_2 = t$, so

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} t \\ t \end{bmatrix} = t \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Thus,

$$P_1 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

is a basis for the eigenvector corresponding to $\lambda = 2$.
Similarly, you can show that

$$\mathrm{P}_2 = \begin{bmatrix} -\frac{1}{4} \\ 1 \end{bmatrix}$$

is a basis for the eigenvector corresponding to $\lambda = -3$. Thus,

$$P = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$$

diagonalizes A, and

$$D = P^{-1}AP = \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix}$$

Thas, as noted in Step 2 of the procedure stated above, the substitution

$$y = Pu \text{ and } y' = P'_{\mathrm{u}}$$

yields the diagonal system"

$$\begin{aligned} u' &= Du \\ &= \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}, \end{aligned}$$

or

$$\begin{aligned} u_1' &= 2u_1 \\ u_2' &= -3u_2 \end{aligned}$$

and the solution of this system is

$$\begin{aligned} u_1 &= c_1 e^{2x} \\ u_2 &= c_2 e^{-1a} \end{aligned} \quad \text{or } u = \begin{bmatrix} c_1 e^{2x} \\ c_2 e^{-3x} \end{bmatrix}$$

so the equation $\mathbf{y} = P\mathbf{u}$ yields, as the solution for $\mathbf{y}$,

$$\begin{aligned} \mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} &= \begin{bmatrix} 1 & -\frac{1}{4} \\ 1 & 1 \end{bmatrix} \begin{bmatrix} c_1 e^{2x} \\ c_2 e^{-3x} \end{bmatrix} \\ &= \begin{bmatrix} c_1 e^{2x} - \frac{1}{4} c_2 e^{-3x} \\ c_1 e^{2x} + c_2 e^{-3x} \end{bmatrix} \end{aligned}$$

or

$$\begin{aligned} y_1 &= c_1 e^{2x} - \tfrac{1}{4} c_2 e^{-3x} \\ y_2 &= c_1 e^{2x} + c_2 e^{-3x} \end{aligned}$$

(b) If we substitute the given initial conditions in the above system, we obtain

$$\begin{aligned} c_1 - \tfrac{1}{4} c_2 &= 1 \\ c_1 + c_2 &= 6 \end{aligned}$$

Solving this system, we obtain $c_1 = 2, c_2 = 4$, so the solution with the initial conditions is

$$\begin{aligned} y_1 &= 2e^{2x} - e^{-3x} \\ y_2 &= 2e^{2x} + 4e^{-3x} \end{aligned}$$

■

3.3 Exercises

1. (a) Solve the system

$$y_1' = y_1 + 4y_2$$
$$y_2' = 2y_1 + 3y_2$$

(b) Find the solution that satisfies the initial conditions $y_1(0) = 0, y_2(0) = 0$

2. (a) Solve the system

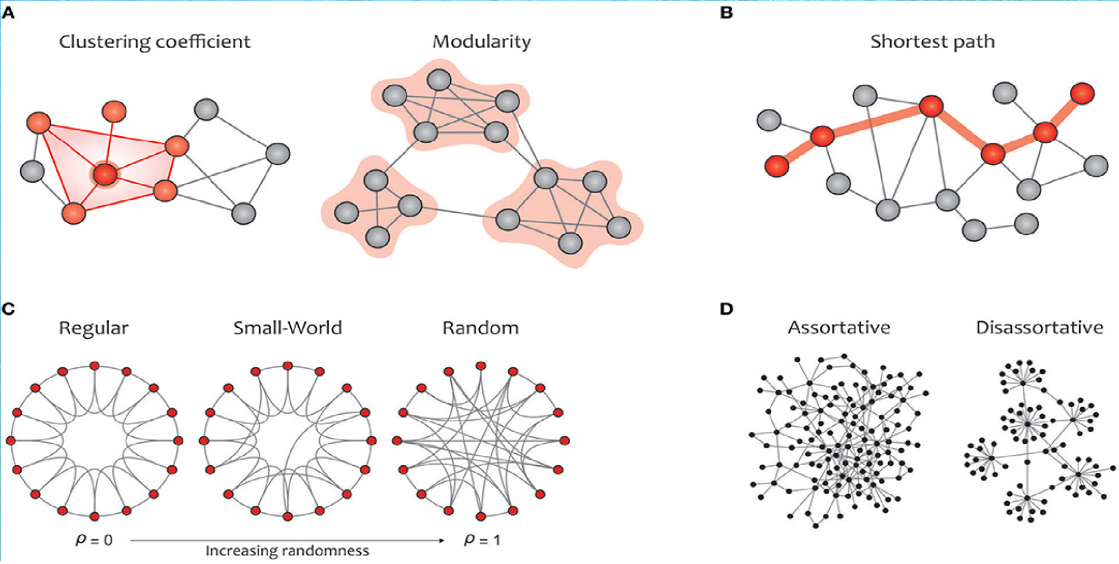
$$y_1' = y_1 + 3y_2$$
$$y_2' = 4y_1 + 5y_2$$

(b) Find the solution that satisfies the conditions $y_1(0) = 2$, $y_2(0) = 1$

3. (a) Solve the system

$$y_1' = 4y_1 \quad + y_3$$
$$y_2' = -2y_1 + y_2$$
$$y_3' = -2y_1 \quad + y_3$$

(b) Find the solution that satisfies the initial conditions $y_1(0) = -1, y_2(0) = 1, y_3(0) = 0$



4. Graph Theory

4.1 Directed Graphs

Definition 4.1.1 A **directed graph** is a finite set of elements, $\{P_1, P_2, ..., P_n\}$, together with a finite collection of ordered pairs (P_i, P_j) of distinct elements of this set, with no ordered pair being repeated. The elements of the set are called **vertices**, and the ordered pairs are called **directed edges**, of the directed graph.

We use the notation $P_i \to P_j$ (which is read "P_i is connected to P_j") to indicate that the directed edge (P_i, P_j) belongs to the directed graph. Geometrically, we can visualize a directed graph by representing the vertices as points in the plane and representing the directed edge $P_i \to P_j$ by drawing a line or arc from vertex P_i to vertex P_j, with an arrow pointing from P_i to P_j. If both $P_i \to P_j$ and $P_j \to P_i$ hold (denoted $P_i \leftrightarrow P_j$), we draw a single line between P_i and P_j with two oppositely pointing arrows. See Figure (4.1)

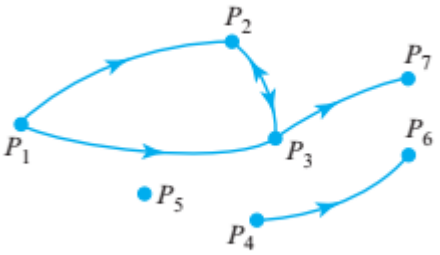


Figure 4.1:

With a directed graph having n vertices, we may associate an $n \times n$ matrix $M = [m_{ij}]$, called **the vertex matrix** of the directed graph. Its elements are defined by

$$m_{ij} = \begin{cases} 1, & \text{if } P_i \to P_j \\ 0, & \text{otherwise} \end{cases}$$

R Vertex matrices have the following two properties:
(i) All entries are either 0 or 1.
(ii) All diagonal entries are 0.
Conversely, any matrix with these two properties determines a unique directed graph having the given matrix as its vertex matrix.

■ **Example 4.1** Find the corresponding vertex matrices for directed graphs in Figure (4.2)
Solution:

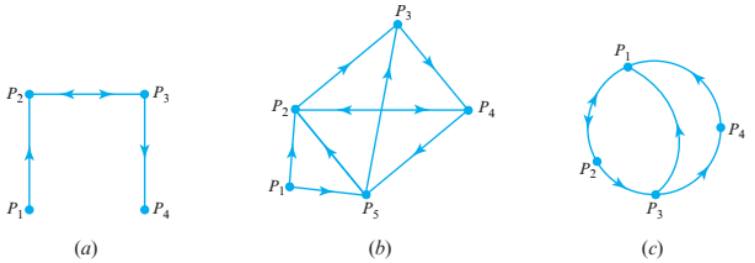


Figure 4.2:

(a)

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

(b)

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

(c)

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

■

■ **Example 4.2** Let M be the vertex matrix define as follow

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

Find the corresponding directed graphs for M.
Solution:
the corresponding directed graphs for M explain in Figure (4.3). ■

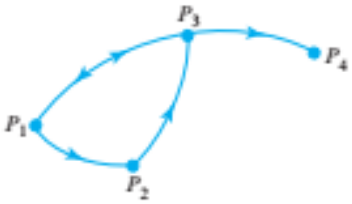


Figure 4.3:

■ **Example 4.3** A certain family consists of a mother, father, daughter, and two sons. The family members have influence, or power, over each other in the following ways: the mother can influence the daughter and the oldest son; the father can influence the two sons; the daughter can influence the father; the oldest son can influence the youngest son; and the youngest son can influence the mother. Find the directed graph and vertex matrix of this model.
Solution:
Figure (4.4) is the resulting directed graph, where we have used obvious letter designations for the five family members.

The vertex matrix of this directed graph is

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

■

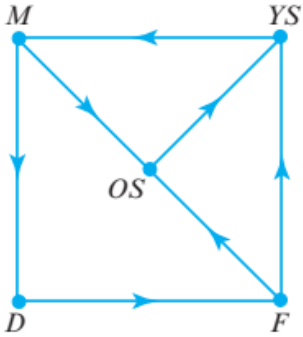


Figure 4.4:

In Example (4.3) the father cannot directly influence the mother; that is, $F \to M$ is not true. But he can influence the youngest son, who can then influence the mother. We write this as $F \to YS \to M$ and call it a 2-step connection from F to M. Analogously, we call $M \to D$ a 1-step connection, $F \to OS \to YS \to M$ a 3-step connection, and so forth.

Now we show a technique for finding the number of all possible r-step connections $(r = 1,2,\ldots)$ from one vertex P_i to another vertex P_j of an arbitrary directed graph.

The number of 1-step connections from P_i to P_j is simply m_{ij}. That is, there is either zero or one 1-step connection from P_i to P_j, depending on whether m_{ij} is zero or one. For the number of 2 -step connections, we consider the square of the vertex matrix. If we let $m_{ij}^{(2)}$ be the (i,j) -th element of M^2, we have

$$m_{ij}^{(2)} = m_{i1}m_{1j} + m_{i2}m_{2j} + \cdots + m_{in}m_{nj}. \tag{4.1}$$

If $m_{i1} = m_{1j} = 1$, there is a 2 -step connection $P_i \to P_1 \to P_j$ from P_i to P_j. But if either m_{i1} or m_{1j} is zero, such a 2 -step connection is not possible. Thus $P_i \to P_1 \to P_j$ is a 2 -step connection if and only if $m_{i1}m_{1j} =$

1. Similarly, for any $k = 1, 2, \ldots, n$, $P_i \to P_k \to P_j$ is a 2-step connection from P_i to P_j if and only if the term $m_{ik}m_{kj}$ on the right side of (4.1) is one; otherwise, the term is zero. Thus, the right side of (4.1) is the total number of two 2 -step connections from P_i to P_j.

In general, we have the following result.

Theorem 4.1.1 Let M be the vertex matrix of a directed graph and let $m_{ij}^{(r)}$ be the (i, j) -th element of M^r. Then $m_{ij}^{(r)}$ is equal to the number of r -step connections from P_i to P_j.

■ **Example 4.4** Figure 4.5 is the route map of a small airline that services the four cities P_1, P_2, P_3, P_4. Find a vertex matrix and r -step connections from P_4 to P_3.

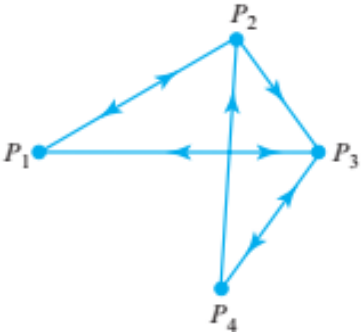


Figure 4.5:

Solution:

As a directed graph, its vertex matrix is

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

We have that

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

and

$$M^3 = \begin{bmatrix} 1 & 3 & 3 & 1 \\ 2 & 2 & 3 & 1 \\ 4 & 0 & 2 & 2 \\ 1 & 3 & 3 & 1 \end{bmatrix}$$

If we are interested in connections from city P_4 to city P_3, by using Theorem 4.1.1 we find their number.
since $m_{43} = 1$, there is one 1-step connection; because $m_{43}^{(2)} = 1$, there is one 2-step connection; and because $m_{43}^{(3)} = 3$, there are three 3-step connections.
Now we verify this, from Figure 3.5 we find
1-step connections from P_4 to P_3 : $P_4 \to P_3$.
2-step connections from P_4 to P_3 : $P_4 \to P_2 \to P_3$.
3-step connections from P_4 to P_3 :

$$P_4 \to P_3 \to P_4 \to P_3.$$
$$P_4 \to P_2 \to P_1. \to P_3$$
$$P_4 \to P_3 \to P_1. \to P_3.$$

■

4.2 cliques

Definition 4.2.1 A subset of a directed graph is called a clique if it satisfies the following three axioms:
(i) The subset contains at least three vertex.
(ii) For each pair of vertices P_i and P_j in the subset, both $P_i \to P_j$ and $P_j \to P_i$ are true.
(iii) The subset is as large as possible; that is, it is not possible to add another vertex the subset and still satisfy condition (ii).

■ **Example 4.5** The directed graph illustrated in Figure 4.6 which might represent the route map of an airline. Find the set of cliques.

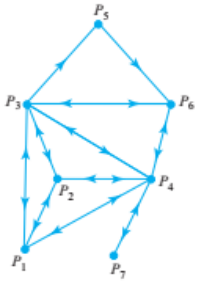


Figure 4.6:

Solution:
The directed graph has two cliques:

$$\{P_1, P_2, P_3, P_4\},$$

and

$$\{P_3, P_4, P_6\}.$$

■

Cliques can be identified by inspecting simple directed graphs. However, a systematic method for detecting cliques in large directed graphs would be ideal. For this reason, t it will be helpful to define a matrix

$$S = [s_{ij}],$$

related to a given directed graph as follows:

$$s_{ij} = \begin{cases} 1, & \text{if } P_i \leftrightarrow P_j \\ 0, & \text{otherwise} \end{cases}$$

The matrix S determines a directed graph that is the same as the given directed graph, with the exception that the directed edges with only one arrow are deleted.

> The matrix S may be obtained from the vertex matrix M of the original directed graph by setting $s_{ij} = 1$ if $m_{ij} = m_{ji} = 1$ and setting $s_{ij} = 0$ otherwise.

The following theorem, which uses the matrix S, is helpful for identifying cliques.

Theorem 4.2.1 Let $s_{ij}^{(3)}$ be the (i, j)-th element of S^3. Then a vertex P_i belongs to some clique if and only if $s_{ii}^{(3)} \neq 0$

Proof. If $s_{ii}^{(3)} \neq 0$, then there is at least one 3-step connection from P_i to itself in the modified directed graph determined by S. Suppose it is $P_i \to P_j \to P_k \to P_i$. In the modified directed graph, all directed relations are two-way, so we also have the connections $P_i \leftrightarrow P_j \leftrightarrow P_k \leftrightarrow P_i$. But this means that $\{P_i, P_j, P_k\}$ is either a clique or a subset of a clique. In either case, P_i must belong to some clique. The converse statement, "if P_i belongs to a clique, then $s_{ii}^{(3)} \neq 0$," follows in a similar manner. ■

■ **Example 4.6** Suppose that a directed graph has as its vertex matrix

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

Find S and show that the directed graph has not clique.
Solution:

$$S = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

and

$$S^3 = \begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{bmatrix}.$$

Because all diagonal entries of S^3 are zero, it follows from Theorem 4.2.1 that the directed graph has no cliques. ■

■ **Example 4.7** Suppose that a directed graph has as its vertex matrix

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

Find S and show that the directed graph has not clique.
Solution:

$$S = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

and

$$S^3 = \begin{bmatrix} 2 & 4 & 0 & 4 & 3 \\ 4 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 2 & 1 \\ 3 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The nonzero diagonal entries of S^3 are $s_{11}^{(3)}, s_{22}^{(3)}$, and $s_{44}^{(3)}$. Consequently, in the given directed graph, P_1, P_2, and P_4 belong to cliques. Because a clique must contain at least three vertices, the directed graph has only one clique, $\{P_1, P_2, P_4\}$. ∎

4.3 Dominance-Directed Graphs

Definition 4.3.1 A dominance-directed graph is a directed graph such that for any distinct pair of vertices P_i and P_j, either $P_i \to P_j$ or $P_j \to P_i$, but not both.

An example of a directed graph satisfying this definition is a league of n sports teams that play each other exactly one time, as in one round of a round-robin tournament in which no ties are allowed. If $P_i \to P_j$ means that team P_i beat team P_j in their single match, it is easy to see that the definition of a dominance-directed group is satisfied. For this reason, dominance-directed graphs are sometimes called **tournaments**.

Theorem 4.3.1 In any dominance-directed graph, there is at least one vertex from which there is a 1-step or 2 -step connection to any other vertex.

Proof. Suppose that a vertex (there may be several) with the largest total number of 1-step and 2-step connections to other vertices in the graph. By renumbering the vertices, we may assume that P_1 is such a vertex. Suppose there is some vertex P_i such that there is no 1-step or 2-step connection from P_1 to P_i. Then, in particular, $P_1 \to P_i$ is not true, so that by definition of a dominance-directed graph, it must be that $P_i \to P_1$. Next, let P_k be any vertex such that $P_1 \to P_k$ is true. Then we cannot have $P_k \to P_i$, as then $P_1 \to P_k \to P_i$ would be a 2-step connection from P_1 to P_i. Thus, it must be that $P_i \to P_k$. That is, P_i has 1-step connections to all the vertices to which P_1 has 1-step connections. The vertex P_i must then also have 2-step connections to all the vertices to which P_1 has 2-step connections.
But because, in addition, we have that $P_i \to P_1$, this means that P_i has more l-step and 2-step connections to other vertices than does P_1. However, this contradicts the way in which P_1 was chosen. Hence, there can be no vertex P_i to which P_1 has no 1-step or 2-step connection. ■

The sum of the entries in the ith row of M is the total number of 1-step connections from P_i to other vertices, and the sum of the entries of the i th row of M^2 is the total number of 2 -step connections from P_i to other vertices. Consequently, the sum of the entries of the i th row of the matrix

$$A = M + M^2,$$

is the total number of 1-step and 2-step connections from P_i to other vertices. In other words, a row of

$$A = M + M^2,$$

with the largest row sum identifies a vertex having the property stated in Theorem 4.3.1

■ **Example 4.8** Suppose that five baseball teams play each other exactly once, and the results are as indicated in the dominance-directed graph of Figure 4.7. Find M and A of the graph.

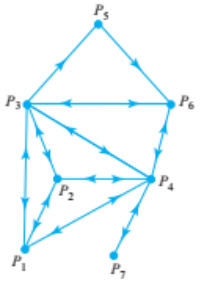


Figure 4.7:

Solution:

The vertex matrix of the graph is

$$M = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix},$$

so

$$A = M + M^2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 3 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 & 2 & 0 \\ 2 & 0 & 3 & 3 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 2 & 3 & 0 \end{bmatrix}.$$

Then the row sums of A are

$$\begin{aligned} \text{1st row sum} &= 4 \\ \text{2nd row sum} &= 9 \\ \text{3rd row sum} &= 2 \\ \text{4th row sum} &= 4 \\ \text{5th row sum} &= 7 \end{aligned}$$

Since the second row has the largest row sum, the vertex P_2 must have a 1-step or 2-step connection to any other vertex. This is easily verified from Figure 3.7. ∎

Definition 4.3.2 The **power** of a vertex of a dominance-directed graph is the total number of 1-step and 2-step connections from it to other vertices. Alternatively, the power of a vertex P_i is the sum of the entries of the i th row of the matrix $A = M + M^2$, where M is the vertex matrix

of the directed graph.

■ **Example 4.9** Let us rank the five baseball teams in Example 4.8 according to their powers. From the calculations for the row sums in that example, we have

$$\begin{gathered}\text{Power of team } P_1 = 4.\\ \text{Power of team } P_2 = 9.\\ \text{Power of team } P_3 = 2.\\ \text{Power of team } P_4 = 4.\\ \text{Power of team } P_5 = 7\end{gathered}$$

Thus, the ranking of the teams according to their powers would be

$$\begin{gathered}\text{First } P_2.\\ \text{Second } P_5.\\ \text{Third } P_1.\\ \text{And tied for thrird } P_4.\\ \text{Last } P_3.\end{gathered}$$

■

4.4 Exercises

A- Draw a diagram of the directed graph corresponding to each of the following vertex matrices.

(a) $\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$.

(b) $\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$.

B- Five baseball teams play each other one time with the following results:

A beats B, C, D
B beats C, E
C beats D, E
D beats B
E beats A, D

Rank the five baseball teams in accordance with the powers of the vertices they correspond to in the dominance-directed graph representing the outcomes of the games.

C- For the dominance-directed graph illustrated in Figure 4.8 construct the vertex matrix and find the power of each vertex

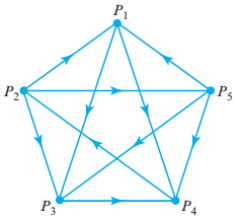
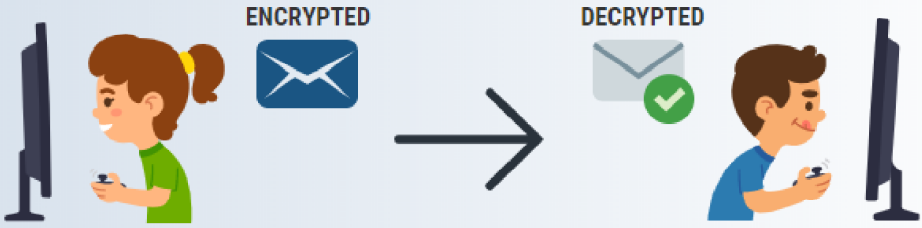


Figure 4.8:



Cryptography Techniques

5. Cryptography

In this chapter, we introduce a method of encoding and decoding messages. Also, we examine modular arithmetic and explaine how Gaussian elimination can sometimes be used to break an opponent's code.

5.1 Ciphers

Secret codes date to the earliest days of written communication, there has been a recent surge of interest in the subject because of the need to maintain the privacy of information transmitted over public lines of communication.

Definition 5.1.1 **Cryptography** is study encoding and decoding of secret messages.

In the language of cryptography:
(i) Codes are called **ciphers**.
(ii) Uncoded messages are called **plaintext**.
(iii) Coded messages are called **ciphertext**.
(iv) The process of converting from plaintext to ciphertext is called **enciphering**.
(v) The reverse process of converting from ciphertext to plaintext is called deciphering.

The simplest ciphers, called substitution ciphers, are those that replace each letter of the alphabet by a different letter.

For example, in the substitution cipher

Plain	A	B	C	D	E	F	J	H	I	J	K	L	M
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P
Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

the plaintext letter A is replaced by D, the plaintext letter B by E, and so forth. With this cipher the plaintext message

ROME WAS NOT BUILT IN A DAY

becomes

URPH ZDV QRW EXLOW LQ D GDB

5.2 Hill Ciphers

In this section we will study a class of polygraphic systems based on matrix transformations.
Now, we assume that each plaintext and ciphertext letter except Z is assigned the numerical value that specifies its position in the standard alphabet (Table 5.1). For reasons that will become clear later, Z is assigned a value of zero.

Plain	A	B	C	D	E	F	J	H	I	J	K	L	M
Cipher	1	2	3	4	5	6	7	8	9	10	11	12	13
Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	14	15	16	17	18	19	20	21	22	23	24	25	0

Table 5.1:

R Whenever an integer greater than 25 occurs, it will be replaced by the remainder that results when this integer is divided by 26. Because the remainder after division by 26 is one of the integers $0, 1, 2, \ldots, 25$, this procedure will always yield an integer with an alphabet equivalent.

In the simplest Hill ciphers, successive pairs of plaintext are transformed into ciphertext by the following procedure:

Step 1. Choose a 2×2 matrix with integer entries

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

to perform the encoding. Certain additional conditions on A will be imposed later.
Step 2. Group successive plaintext letters into pairs, adding an arbitrary "dummy" letter to fill out the last pair if the plaintext has no odd number of letters, and replace each plaintext letter by its numerical value.
Step 3. Successively convert each plaintext pair

$$P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

into a column vector and form the product AP. We will call P a plaintext vector and AP the corresponding ciphertext vector.
Step 4. Convert each ciphertext vector into its alphabetic equivalent.

■ **Example 5.1** Use the matrix

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

to obtain the Hill cipher for the plaintext message

I AM HIDING

Solution:
If we group the plaintext into pairs and add the dummy letter G to fill out the last pair, we obtain

$$IA \quad MH \quad ID \quad IN \quad GG$$

Form Table 5.1, we find

$$9 \quad 1 \quad 13 \quad 8 \quad 9 \quad 4 \quad 9 \quad 14 \quad 7 \quad 7$$

To encipher the pair IA, we form the matrix product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}.$$

From Table 5.1 , yields the ciphertext KC. To encipher the pair MH, we form the product

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 13 \\ 8 \end{bmatrix} = \begin{bmatrix} 29 \\ 24 \end{bmatrix}$$

However, there is a problem here, because the number 29 has no alphabet equivalent (Table 5.1). To resolve this problem, we use the above remark. Thus, we replace 29 by 3, which is the remainder after dividing 29 by 26. It now follows from Table 5.1 that the ciphertext for the pair MH is CX. The computations for the remaining ciphertext vectors are

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 12 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 14 \end{bmatrix} = \begin{bmatrix} 37 \\ 42 \end{bmatrix} \text{ or } \begin{bmatrix} 11 \\ 16 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 7 \end{bmatrix} = \begin{bmatrix} 21 \\ 21 \end{bmatrix}$$

These correspond to the ciphertext pairs QL, KP, and UU, respectively. Therefore, the entire ciphertext message is

$$KC \quad CX \quad QL \quad KP \quad UU$$

which, in most situations, will be sent as a single string with no spaces:

KCCXQLKPUU

■

- The Hill cipher in Example 5.1 is referred to as a Hill 2-cipher because the plaintext was grouped in pairs and enciphered by a 2×2 matrix.

- The plaintext can also be divided into triples and enciphered using a 3×3 matrix of integer entries, which is known as a Hill 3-cipher.
- In general, for a Hill n-cipher, plaintext is grouped into sets of n letters and enciphered by an $n \times n$ matrix with integer entries.

5.3 Modular Arithmetic

A positive integer m is called the modulus in modular arithmetic, and any two integers whose difference is an integer multiple of the modulus are treated as "equal" or "equivalent" with respect to the modulus. To be more specific, we include the following definition.

Definition 5.3.1 If m is a positive integer and a and b are any integers, then we say that a is equivalent to b modulo m, written

$$a = b \pmod{m},$$

if $a - b$ is an integer multiple of m.

■ **Example 5.2**

$$\begin{aligned} 7 &= 2 \pmod{5} \\ 19 &= 3 \pmod{2} \\ -1 &= 25 \pmod{26} \\ 12 &= 0 \pmod{4} \end{aligned}$$

■

For any modulus m it ean be proved that every integer a is equivalent, modulo m, to exactly one of the integers

$$0, 1, 2, \ldots, m-1$$

We call this integer the residue of a modulo m, and we write

$$Z_n = \{0, 1, 2, \ldots, m-1\}$$

to denote the set of residues modulo m. If a is a non-negative integer, then its residue modulo m is simply the remainder that results when a is divided by m.
The residue can be found using the following theorem for any integer a.

Theorem 5.3.1 For any integer a and modulus m, let

$$R = \text{ remainder of } \frac{|a|}{m}$$

Then the residue r of a modulo m is given by

$$r = \begin{cases} R & \text{if } a \geq 0 \\ m - R & \text{if } a < 0 \text{ and } R \neq 0 \\ 0 & \text{if } a < 0 \text{ and } R = 0 \end{cases}$$

■ **Example 5.3** Find the residue modulo 26 of
(a) 87,
$(b) -38$,
$(c) -26$.
Solution:
(a) Dividing $|87| = 87$ by 26 yields a remainder of $R = 9$, so $r = 9$. Thus,

$$87 = 9 \pmod{26}.$$

(b) Dividing $|-38| = 38$ by 26 yields a remainder of $R = 12$, so $r = 26 - 12 = 14$. Thus

$$-38 = 14 \pmod{26}.$$

(c) Dividing $|-26| = 26$ by 26 yields a remainder of $R = 0$. Thus,

$$-26 = 0 \pmod{26}.$$

■

The next definition explain the multiplicative inverse.

Definition 5.3.2 If a is a number in Z_m , then number Z_m is called a reciprocal or multiplicative inverse of a modulo m if $aa^{-1} = a^{-1}a = 1 \pmod{m}$.

R It can be proved that if a and m have no common prime factors, then a has a unique reciprocal modulo m; conversely, if a and m have a common prime factor, then a has no reciprocal modulo m.

■ **Example 5.4** The number 3 has multiplicative inverse in modulo 26 because 3 and 26 have no common prime factors. This multiplicative inverse can be obtained by finding the number x in Z_{26} that satisfies the modular equation

$$3x = 1 \pmod{26}.$$

Although there are general methods for solving such modular equations, it would take us too far afield to study them. However, because 26 is relatively small, this equation can be solved by trying the possible solutions, 0 to 25, one at a time. With this approach we find that $x = 9$ is the solution, because

$$3 \cdot 9 = 27 = 1 \pmod{26}.$$

Thus,

$$3^{-1} = 9 \quad (\text{mod.}$$

■

■ **Example 5.5** The number 4 has no multiplicative inverse in modulo 26, because 4 and 26 have 2 as a common prime factor ■

For future reference, in Table 5.2 we provide the following multiplicative inverse in modulo 26:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Table 5.2: multiplicative inverse in Modulo 26

5.4 Deciphering

Every useful cipher must have a procedure for decipherment. In the case of a Hill cipher, decipherment uses the inverse (mod 26) of the enciphering matrix. To be precise, if m is a positive integer, then a square matrix A with entries in Z_m is said to be invertible modulo m if there is a matrix B with entries in Z_{m} such that

$$AB = BA = I \pmod{m}.$$

Assume that

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

is invertible modulo 26 and this matrix is used in a Hill 2-cipher. If

$$\mathbf{p} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix},$$

is a plaintext vector, then

$$c = Ap \pmod{26},$$

is the corresponding ciphertext vector and

$$\mathbf{p} = A^{-1}\mathbf{c} \pmod{26}.$$

Thus, each plaintext vector can be recovered from the corresponding ciphertext vector by multiplying it on the left by $A^{-1} \pmod{26}$.

It's crucial to know which matrices are modulo 26 invertible and how to get their inverses in cryptography. We're now looking into these questions.

In ordinary arithmetic, a square matrix A is invertible if and only if $\det(A) \neq 0$.
Now, the following theorem is the analog of this result in modular arithmetic.

Theorem 5.4.1 A square matrix A with entries in Z_m is invertible modulo m if and only if the residue of det(A) modulo m has a multiplicative inverse in modulo m.

Since the residue of $\det(A)$ modulo m will have a multiplicative inverse in modulo m if and only if this residue and m have no common prime factors, then we have the following corollary.

Corollary 5.4.2 A square matrix A with entries in Z_m is invertible modulo m if and only if m and the residue of det(A) modulo m have no common prime factors.

The following corollary is useful in cryptography since the only prime factors of $m = 26$ are 2 and 13.

Corollary 5.4.3 A square matrix A with entries in Z_{26} is invertible modulo 26 if and only if the residue of $\det(A)$ modulo 26 is not divisible by 2 or 13.

It easy to verify that if

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

has entries in Z_{26} and the residue of $det(A) = ad - bc$ modulo 26 is not divisible by 2 or 13, then the inverse of A (mod 26) is given by

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \ (mod\ 26), \tag{5.1}$$

where $(ad - bc)^{-1}$ is the inverse of the residue of $ad - bc$ (mod 26).

■ **Example 5.6** Find the inverse of

$$A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix},$$

modulo 26.
Solution:

$$\det(A) = ad - bc = 5 \cdot 3 - 6 \cdot 2 = 3$$

so from Table 5.2.

$$(ad - bc)^{-1} = 3^{-1} = 9 (\bmod 26)$$

Thus, from (5.1),

$$\begin{aligned} A^{-1} &= 9 \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} \\ &= \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \quad (\bmod 26). \end{aligned}$$

As a check,

$$\begin{aligned} AA^{-1} &= \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \\ &= \begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (\text{mod} 26). \end{aligned}$$

Similarly, $A^{-1}A = I$. ∎

∎ **Example 5.7** Decode the following Hill 2 -cipher, which was enciphered by the matrix in Example 5.6

GTNKGKDUSK

Solution: From Table 5.1 the numerical equivalent of this ciphertext is

7 20 14 11 7 11 4 21 19 11

To obtain the plaintext pairs, we multiply each ciphertext vector by the inverse of (obtained in Example 5.6):

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 20\end{bmatrix} = \begin{bmatrix}487\\ 436\end{bmatrix} = \begin{bmatrix}19\\ 20\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}14\\ 11\end{bmatrix} = \begin{bmatrix}278\\ 321\end{bmatrix} = \begin{bmatrix}18\\ 9\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}7\\ 11\end{bmatrix} = \begin{bmatrix}271\\ 265\end{bmatrix} = \begin{bmatrix}11\\ 5\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}4\\ 21\end{bmatrix} = \begin{bmatrix}508\\ 431\end{bmatrix} = \begin{bmatrix}14\\ 15\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}1 & 24\\ 8 & 19\end{bmatrix}\begin{bmatrix}19\\ 11\end{bmatrix} = \begin{bmatrix}283\\ 361\end{bmatrix} = \begin{bmatrix}23\\ 23\end{bmatrix} \pmod{26}$$

Figure 5.1:

From Table 5.1, the alphabet equivalents of these vectors are

$$ST \quad RI \quad KE \quad NO \quad WW$$

which yields the message

STRIKE NOW

■

5.5 Breaking a Hill Cipher

Cryptographers are concerned with the security of their ciphers—that is, how easily they can be broken—because the aim of encrypting messages and information is to prevent "opponents" from knowing their contents (deciphered by their opponents). We'll wrap up this section with a look at one approach for cracking Hill ciphers.

Assume you can able to obtain any associated plaintext and ciphertext from an opponent's message. Examining any intercepted ciphertext, for example, you may be able to deduce that the message is a letter that starts with DEAR SIR. We'll demonstrate how, given a small amount of such data, it's possible to deduce a Hill code's deciphering matrix and thus gain access to the rest of the message.

The fact that a linear transformation is absolutely determined by its values at a basis is a fundamental result in linear algebra. According to this theory, if we have a Hill n-cipher, and if

$$P_1 \quad P_2 \quad \ldots \quad P_n$$

are linearly independent plaintext vectors whose corresponding ciphertext vectors

$$AP_1 \quad AP_2 \quad \ldots \quad AP_n$$

are known, then there is enough information available to determine the matrix A and hence A^{-1} (mod m).

The next theorem tells us that to find the transpose of the deciphering matrix A^{-1}, we must find a sequence of row operations that reduces C to I and then perform this same sequence of operations on P.

Theorem 5.5.1 Let $\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n$ be linearly independent plaintext vectors, and let $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ be the corresponding ciphertext vectors in a Hill n-cipher. If

$$P = \begin{bmatrix} \mathbf{p}_1^T \\ \mathbf{p}_2^T \\ \vdots \\ \mathbf{p}_n^T \end{bmatrix}$$

is the $n \times n$ matrix with row vectors $\mathbf{p}_1^T, \mathbf{p}_2^T, \ldots, \mathbf{p}_n^T$ and if

$$C = \begin{bmatrix} \mathbf{c}_1^T \\ \mathbf{c}_2^T \\ \vdots \\ \mathbf{c}_n^T \end{bmatrix}$$

is the $n \times n$ matrix with row vectors $\mathbf{c}_1^T, \mathbf{c}_2^T, \ldots, \mathbf{c}_n^T$, then the sequence of elementary row operations that reduces C to I transforms P to $\left(A^{-1}\right)^T$.

The following example illustrates a simple algorithm for doing this.

■ **Example 5.8** The following Hill 2-cipher is intercepted:

IOSBTGXESPXHOPDE

Decipher the message, given that it starts with the word *DEAR*.
Solution:
Since the numerical equivalent of the known plaintext is

D	E	A	R
4	5	1	18

and the numerical equivalent of the corresponding ciphertext is

I	O	S	B
9	15	19	2

so the corresponding plaintext and ciphertext vectors are

$$\mathbf{p}_1 = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \leftrightarrow \mathbf{c}_1 = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$
$$\mathbf{p}_2 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \leftrightarrow \mathbf{c}_2 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

We want to reduce

$$C = \begin{bmatrix} \mathbf{c}_1^T \\ \mathbf{c}_2^T \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$$

to I by elementary row operations and simultaneously apply these operations to

$$P = \begin{bmatrix} \mathbf{p}_1^T \\ \mathbf{p}_2^T \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$$

to obtain $\left(A^{-1}\right)^T$. It is possible to do this.by adjoining P to the right of C and applying row operations to the resulting matrix $[C \mid P]$ until the left side is reduced to I. The final matrix will then have the form

$$\left[I \mid \left(A^{-1}\right)^T\right].$$

The computations can be carried out as follows:

$$\left[\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right] \overset{9^{-1}r_1 = 3r_1}{\rightarrow}$$

$$\left[\begin{array}{cc|cc} 1 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right] \rightarrow$$

We replaced 45 by its residue modulo 26.

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right] \overset{-19r_1 + r_2}{\rightarrow}$$

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right] \rightarrow$$

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{array}\right] \overset{5^{-1}r_2=21r_2}{\rightarrow}$$

$$\left[\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right] \overset{-19r_2+r_2}{\rightarrow}$$

$$\left[\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right] \rightarrow$$

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right].$$

Thus,

$$\left(A^{-1}\right)^T = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix},$$

so the deciphering matrix is

$$A^{-1} = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix},$$

To decipher the message, we first group the ciphertext into pairs and find the numerical equivalent of each letter:

IO	*SB*	*TG*	*XE*	*SP*	*XH*	*OP*	*DE*
915	192	207	245	1916	248	1516	45

Next, we multiply successive ciphertext vectors on the left by A^{-1} and find the alphabet equivalents of the resulting plaintext pairs:

$$
\begin{aligned}
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}9\\ 15\end{bmatrix} &= \begin{bmatrix}4\\ 5\end{bmatrix} && D\ E\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}19\\ 2\end{bmatrix} &= \begin{bmatrix}1\\ 18\end{bmatrix} && A\ R\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}20\\ 7\end{bmatrix} &= \begin{bmatrix}9\\ 11\end{bmatrix} && I\ K\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}24\\ 5\end{bmatrix} &= \begin{bmatrix}5\\ 19\end{bmatrix} && E\ S\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}19\\ 16\end{bmatrix} &= \begin{bmatrix}5\\ 14\end{bmatrix} && E\ N\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}24\\ 8\end{bmatrix} &= \begin{bmatrix}4\\ 20\end{bmatrix} && D\ T\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}15\\ 16\end{bmatrix} &= \begin{bmatrix}1\\ 14\end{bmatrix} && A\ N\\
\begin{bmatrix}1 & 17\\ 0 & 9\end{bmatrix}\begin{bmatrix}4\\ 5\end{bmatrix} &= \begin{bmatrix}11\\ 19\end{bmatrix} && K\ S
\end{aligned}
\pmod{26}
$$

Figure 5.2:

Finally, we construct the message from the plaintext pairs:

DE AR IK ES EN DT AN KS
DEARIKE SEND TANKS

■

5.6 Exercise

1. Obtain the Hill cipher of the message

DARK NIGHT

for each of the following enciphering matrices:

(a) $\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$.

(b) $\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$.

2. In each part determine whether the matrix is invertible modulo 26. If so, find its inverse modulo 26 and check your work by verifying that

$$AA^{-1} = A^{-1}A = I(\bmod 26)$$

(a) $A = \begin{bmatrix} 9 & 1 \\ 7 & 2 \end{bmatrix}$

(b) $A = \begin{bmatrix} 3 & 1 \\ 5 & 3 \end{bmatrix}$

(c) $A = \begin{bmatrix} 8 & 11 \\ 1 & 9 \end{bmatrix}$

(d) $A = \begin{bmatrix} 2 & 1 \\ 1 & 7 \end{bmatrix}$

(e) $A = \begin{bmatrix} 3 & 1 \\ 6 & 2 \end{bmatrix}$

(f) $A = \begin{bmatrix} 1 & 8 \\ 1 & 3 \end{bmatrix}$

3. Decode the message

SAKNOXAOJX

given that it is a Hill cipher with enciphering matrix

$$\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$$

4. A Hill 2 -cipher is intercepted that starts with the pairs

$$SLHK$$

Find the deciphering and enciphering matrices, given that the plaintext is known to start with the word *ARMY*.

5. Decode the following Hill 2 -cipher if the last four plaintext letters are known to be *ATOM*.

LNGIHGYBVRENJYQO

Wish you all the best, Dr. A. Elrawy