MATH 146: Linear Algebra 1

Instructor: Ross Willard & Giang Tran

Winter 2021

Table of Contents

Chapter 4: Determinants

4.1 Definition of the determinant

4.2 Basic properties of determinants

4.3 Determinants, invertibility, products, and transposes

4.4 Other Cofactor Expansions

4.5 A formula for the inverse of a matrix and the Leibniz expansion of determinants

4.6 Summary–Important Facts About Determinants

Chapter 5: Diagonalization

5.1 Eigenvalues and Eigenvectors

5.2 Diagonalization

5.3 The Cayley-Hamilton Theorem

1 Vector Spaces

1.1 Definitions and Examples

Definition 1 (Fields). *A field $\mathbb{F}$ is a set on which two operations*

- *addition,* $\mathbb{F} \times \mathbb{F} \to \mathbb{F}, \quad (a, b) \mapsto a + b$ *(the sum of a and b),*
- *multiplication,* $\mathbb{F} \times \mathbb{F} \to \mathbb{F}, \quad (a, b) \mapsto a \cdot b$ *(the product of a and b),*

are defined, and such that the following conditions hold for all elements $a, b, c \in \mathbb{F}$:

(F 1) $a + b = b + a$ *and* $a \cdot b = b \cdot a$ *(Commutativity of addition and multiplication).*

(F 2) $(a+b)+c = a+(b+c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Associativity of addition and multiplication).*

(F 3) There exist distinct elements 0 and 1 in $\mathbb{F}$ such that

$$0 + a = a \quad \text{and} \quad 1 \cdot a = a$$

(Existence of identity elements for addition and multiplication).

(F 4) For each element $a \in \mathbb{F}$, there exists an element $c \in \mathbb{F}$, called an additive inverse for a, such that $a + c = 0$; and for each nonzero element $b \in \mathbb{F} \setminus \{0\}$, there exists an element $d \in \mathbb{F}$, called a multiplicative inverse for b, such that $b \cdot d = 1$ (Existence of inverses for addition and multiplication).

(F 5) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(Distributivity of multiplication over addition).*

Remark 1. Roughly speaking, a field is a set

1. Containing distinct elements 0, 1, and possibly others,
2. Having four operations (addition, multiplication, subtraction, and division) so that, with the exception of division by zero, the sum, product, difference, and quotient of any two elements in the set is an element of the set,
3. Satisfying the "obvious" algebraic laws (commutativity, associativity, distributivity, existence of identities and inverses elements for addition and multiplication).

Example 1. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are fields. For each prime p, $\mathbb{Z}_p$ is a field. $\mathbb{Z}$ is not a field. If $n > 0$ is not a prime, then $\mathbb{Z}_n$ is not a field.

Throughout this section, we denote $\mathbb{F}$ a field.

Definition 2 (Vector Spaces). *A vector space over a field $\mathbb{F}$ is a set V on which two operations*

- *addition,* $V \times V \to V, \quad (x, y) \mapsto x + y$ *(the sum of x and y),*
- *scalar multiplication,* $\mathbb{F} \times V \to V, \quad (a, x) \mapsto ax$ *(the product of a and x),*

are defined, and such that the following conditions hold for all elements $x, y, z \in V$ and $a, b \in \mathbb{F}$:

(VS 1) $x + y = y + x$.

(VS 2) $(x + y) + z = x + (y + z)$.

(VS 3) *There exists a zero vector, 0, in* V *such that* $x + 0 = x$.

(VS 4) *For each element* $x \in V$, *there exists an element* $y \in V$, *called an additive inverse for* x, *such that* $x + y = 0$.

(VS 5) $1x = x$.

(VS 6) $(ab)x = a(bx)$.

(VS 7) $a(x + y) = ax + ay$.

(VS 8) $(a + b)x = ax + bx$.

The elements of the field $\mathbb{F}$ *are called scalars and the elements of the vector space* V *are called vectors.*

Remark 2. The condition (VS 2) allows us to define the addition of any finite number of vectors (without the use of parentheses). The conditions (VS 1) and (VS 2) permit us to perform the additions in any order. For example, we have

$$((x + y) + z) + w = (x + (y + z)) + w = ((y + z) + x) + w = (y + z) + (x + w), \quad \text{etc},$$

which we write simply as $x + y + z + w$.

Throughout this chapter, a vector space is frequently discussed without explicitly mentioning its field of scalars. That is, a vector space V means a vector space V over a given field $\mathbb{F}$. Now, we present four standard examples of vector spaces.

Example 2. Denote $\mathbb{F}^n$ the set of n-tuples with entries (components) from the field $\mathbb{F}$,

$$\mathbb{F}^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{F}\}.$$

Two elements of $\mathbb{F}^n$,

$$a = (a_1, \ldots, a_n) \quad \text{and} \quad b = (b_1, \ldots, b_n),$$

are said to be equal if $a_k = b_k$ for $k = 1, \ldots n$.

Claim: The set $\mathbb{F}^n$ is a vector space over $\mathbb{F}$ with the operations of coordinate-wise addition and scalar multiplication:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n),$$

$$c(a_1, \ldots, a_n) := (ca_1, \ldots, ca_n),$$

for all $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{F}^n$ and for all $c \in \mathbb{F}$. Vectors in $\mathbb{F}^n$ may be written as column vectors

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad \text{or} \quad \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}.$$

Proof sketch. Clearly, the two operations are well-defined. We need to verify all eight conditions of a vector space. We will check (VS 3). The zero element of $\mathbb{F}^n$ is the n-tuple

$$0 = (0, \ldots, 0),$$

with all its entries equal to 0. Suppose $a = (a_1, \ldots, a_n) \in \mathbb{F}^n$. Then

$$\begin{aligned} a + 0 &= (a_1, \ldots, a_n) + (0, \ldots, 0) \\ &= (a_1 + 0, \ldots, a_n + 0) \quad \text{(definition of } + \text{ in } \mathbb{F}^n) \\ &= (a_1, \ldots, a_n) \quad \text{(property of the additive identity element)} \\ &= a. \end{aligned}$$

Verifying the remaining conditions are left to students. □

Remark 3. From Example 2, we conclude that $\mathbb{Q}^n$ is a vector space over $\mathbb{Q}$, $\mathbb{R}^n$ is a vector space over $\mathbb{R}$, and $\mathbb{C}^n$ is a vector space over $\mathbb{C}$. Note that $\mathbb{Q}^n$ is not a vector space over $\mathbb{R}$ and $\mathbb{R}^n$ is not a vector space over $\mathbb{C}$.

On the other hand, $\mathbb{R}^n$ *can* be considered a vector space over $\mathbb{Q}$ - roughly because we can multiply vectors in $\mathbb{R}^n$ by scalars from $\mathbb{Q}$ and the result is always still a vector in $\mathbb{R}^n$. Similarly, $\mathbb{C}^n$ can be viewed as a vector space over $\mathbb{R}$. Note that $\mathbb{C}^n$ viewed as a vector space over $\mathbb{R}$ is *not* the same as $\mathbb{C}^n$ viewed as a vector space over $\mathbb{C}$. For example, we will define the notion of *dimension* in week 3, and then it will be easy to see that $\mathbb{C}^n$ as a vector space over $\mathbb{C}$ has dimension n, while $\mathbb{C}^n$ as a vector space over $\mathbb{R}$ has dimension $2n$. Similarly, $\mathbb{R}^n$ as a vector space over $\mathbb{R}$ will have dimension n, while $\mathbb{R}^n$ as a vector space over $\mathbb{Q}$ will be infinite-dimensional (technically, it will have dimension equal to the continuum, though we will not prove this).

Generally, whenever we talk about "the" vector space $\mathbb{F}^n$ we mean $\mathbb{F}^n$ considered as a vector space over $\mathbb{F}$.

Definition 3 (Matrices)**.** *Let $\mathbb{F}$ be a field. Let m, n be two fixed integers ≥ 1.*

- *An $m \times n$ matrices with entries from a field $\mathbb{F}$ is a rectangular array of the form*

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix},$$

  where $a_{ij} \in \mathbb{F}$ for $1 \leq i \leq m, 1 \leq j \leq n$. We can abbreviate the notation for this matrix by writing it $(a_{ij}), i = 1, \ldots, m$ and $j = 1, \ldots, n$. We call a_{ij} the ij-entry of the matrix, i.e, entry at the i-th row and the j-th column.

- *The $m \times n$ matrix in which each entry equals zero is called the zero matrix and is denoted by O.*

- *Two $m \times n$ matrices $A = (a_{ij})$ and $B = (b_{ij})$ are said to be equal if all their corresponding entries are equal, that is, if $a_{ij} = b_{ij}$, for all $1 \leq i \leq m, 1 \leq j \leq n$.*

- *(Matrix Addition) Let $A = (a_{ij})$ and $B = (b_{ij})$ be two $m \times n$ matrices with entries from $\mathbb{F}$. We define $A + B$ to be an $m \times n$ matrix whose entry in the i-th row and j-th column is $a_{ij} + b_{ij}$, that is,*

$$(A + B)_{ij} := a_{ij} + b_{ij},$$

for all $1 \leq i \leq m, 1 \leq j \leq n$.

- *(Scalar Multiplication) Let $A = (a_{ij})$ be an $m \times n$ matrix with entries from $\mathbb{F}$ and $c \in \mathbb{F}$. We define cA to be an $m \times n$ matrix whose entry in the i-th row and j-th column is ca_{ij}.*

Example 3 (The Space of Matrices)**.** Denote $\mathbf{M}_{m\times n}(\mathbb{F})$ the set of all $m \times n$ matrices with entries from the field $\mathbb{F}$. Then the set $\mathbf{M}_{m\times n}(\mathbb{F})$ with the above matrix addition and scalar multiplication is a vector space over $\mathbb{F}$. (Proof is left as an exercise).

Example 4 (Function Spaces)**.** Let D be any nonempty set and $\mathbb{F}^D$ be the set of all functions from D to $\mathbb{F}$. The set $\mathbb{F}^D$ is a vector space with the following operations:

$$(f + g)(x) := f(x) + g(x) \quad \text{and} \quad (cf)(x) := cf(x), \quad x \in D,$$

for all $f, g \in \mathbb{F}^D$ and $c \in \mathbb{F}$.

Definition 4 (Polynomials)**.** *A polynomial with coefficients from a field $\mathbb{F}$ is an expression of the form*

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

where n is a nonnegative integer, $a_k \in \mathbb{F}$ for $0 \leq k \leq n$ (called the coefficient of x^k), and x is a variable.

- *The polynomial in which all coefficients are zero is called the zero polynomial, $f(x) = 0$.*
- *Two polynomials with coefficients from a field $\mathbb{F}$,*

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

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

are said to be equal, if $m = n$ and $a_k = b_k$ for $0 \leq k \leq n$.

- *Denote $\mathrm{P}_n(\mathbb{F})$ the set of all polynomials of degree at most n.*

$$\mathrm{P}_n(\mathbb{F}) = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_0, \ldots, a_n \in \mathbb{F}\}.$$

- *Denote $\mathbb{F}[x]$ the set of all polynomials (of all degrees) with coefficients from $\mathbb{F}$.*
- *(Polynomial Addition) Let $f, g \in \mathbb{F}[x]$,*

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

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

where $a_k, b_j \in \mathbb{F}$, for $0 \leq k \leq n$ and $0 \leq j \leq m$. Without loss of generality, assume $n \geq m$. Then we can write $b_j = 0$ for $j > m$,

$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0,$$

and we define the sum $f + g$ as

$$(f + g)(x) := (a_n + b_n)x^n + \cdots + (a_0 + b_0).$$

Then $f + g \in \mathbb{F}[x]$.

- *(Scalar Multiplication) Let $f \in \mathbb{F}[x]$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, and $c \in \mathbb{F}$. We define $cf \in \mathbb{F}[x]$ as*

$$(cf)(x) := ca_n x^n + \cdots + ca_0.$$

Example 5 (The Space of Polynomials)**.** The set $\mathbb{F}[x]$ with the above operations of addition and scalar multiplication is a vector space over $\mathbb{F}$.

Next, we present some sets on which addition and scalar multiplication are defined, but which are not vector spaces.

Example 6. Let $S = \{(a_1, a_2) \mid a_1, a_2 \in \mathbb{R}\}$. For $(a_1, a_2), (b_1, b_2) \in S$ and $c \in \mathbb{R}$, we define

$$(a_1, a_2) + (b_1, b_2) := (2a_1 + b_1, a_2 + b_2) \quad \text{and} \quad c(a_1, a_2) := (ca_1, ca_2).$$

Then S is not a vector space under these operations since (VS 1) fails.

Example 7. Let $S = \{(a_1, a_2) \in \mathbb{R}^2 \mid a_1 \geq 0\}$ as in $\mathbb{R}^2$. Then S is not a vector space over $\mathbb{R}$ (at least, under the standard addition and scalar multiplication) since scalar multiplication is not a well-defined operation, in the following sense: if we take $a = (1, 3) \in S$ and let $c = -1 \in \mathbb{R}$, then ca should be an element in S, but it is not.

1.2 Basic Properties

Theorem 1.1 (Cancellation Law for Vector Addition)**.** *Let V be a vector space. If $x, y, z \in V$ such that $x + z = y + z$, then $x = y$.*

Proof. Assume that $x + z = y + z$. Then

$$\begin{aligned}
x &= x + 0 && \text{by (VS 3)} \\
&= x + (z + v) && \text{where } v \text{ is an additive inverse for } z \text{ as promised in (VS 4)} \\
&= (x + z) + v && \text{by (VS 2)} \\
&= (y + z) + v && \text{assumption: } x + z = y + z \\
&= y + (z + v) && \text{by (VS 2)} \\
&= y + 0 && \text{by the choice of } v \text{ in line 2} \\
&= y && \text{by (VS 3).}
\end{aligned}$$

□

Corollary 1.1.1. Let V be a vector space and $x \in V$.

1. There is exactly one vector in V that can be the zero vector.
2. There is exactly one vector $y \in V$ such that $x + y = 0$.

Proof. 1. Suppose the vectors $0_1 \in V$ and $0_2 \in V$ both satisfy the property in (VS 3). Then for any $x \in V$ we have

$$\begin{aligned}
0_1 + x &= x + 0_1 && \text{by (VS 1)} \\
&= x && \text{assumption: } 0_1 \text{ satisfies (VS 3)}
\end{aligned}$$

A similar argument gives $0_2 + x = x$. Therefore $0_1 + x = 0_2 + x$. Now use the Cancellation Law to get $0_1 = 0_2$. This proves that we can't have more than one element of V satisfying (VS 3).

2. The proof is similar to the proof of (1). Assuming that $x \in V$ has two inverses y_1 and y_2 (i.e., both y_1 and y_2 satisfy (VS 4) for x), we can use (VS 1) and the assumption to argue that $y_1 + x = y_2 + x$ (they both equal 0), so by the Cancellation Law, $y_1 = y_2$.

□

Definition 5. *Let V be a vector space and $x, z \in V$.*

- *Denote $-x$ the unique vector $y \in V$ such that $x + y = 0$.*
- *Denote $x - z$ the sum $x + (-z)$.*

Theorem 1.2. *Let V be a vector space over $\mathbb{F}$, $x \in V$, and $a \in \mathbb{F}$. Then we have the following:*

1. $0x = 0$.
2. $a0 = 0$.
3. $(-a)x = -(ax) = a(-x)$. *In particular,* $(-1)x = -x$.

Remark. Note the overloaded notation in the statement. For example, in part (1), the first 0 is the scalar $0 \in \mathbb{F}$, while the second 0 is the zero vector in V. In part (2), the first $-$ means minus in $\mathbb{F}$, while the second and third mean the minus in V defined above in Definition 5.

Proof. We will prove (1) and (2) in the recorded modules. Here is a proof of (3). For any $a \in \mathbb{F}$ and $x \in V$ we have

$$\begin{aligned} ax + (-a)x &= (a + -a)x && \text{(VS 8)} \\ &= 0x && \text{arithmetic in } \mathbb{F} \\ &= 0 && \text{Theorem 1.2 part 1} \end{aligned}$$

which implies that $(-a)x$ satisfies the property in (VS 3) for being an additive inverse of ax. Since ax has only one additive inverse by Corollary 1.1.1 part 2, which we denote by $-(ax)$ as stated in Definition 5, this prove that $(-a)x = -(ax)$.
We also have

$$\begin{aligned} ax + a(-x) &= a(x + -x) && \text{(VS 7)} \\ &= a0 && -x \text{ by definition is the additive inverse of } x \\ &= 0 && \text{Theorem 1.2 part 2.} \end{aligned}$$

which implies $a(-x) = -(ax)$ by similar logic. □

1.3 Subspaces

Definition 6. *A subset W of a vector space V over a field $\mathbb{F}$ is called a subspace of V if the following three conditions hold for the operations defined in V:*

(S 1) $W \neq \emptyset$.

(S 2) If $x \in W$ *and* $y \in W$, *then* $x + y \in W$.

(S 3) If $c \in \mathbb{F}$ *and* $x \in W$, *then* $cx \in W$.

Theorem 1.3. *If W is a subspace of a vector space V over a field $\mathbb{F}$, then W is a vector space over $\mathbb{F}$ under the operations of V restricted to W.*

Proof Sketch. We need to check all 8 conditions of vector spaces. Since all conditions except (VS 3) and (VS 4) hold for all $x, y, z \in V$, because $W \subset V$, and because we use the same operations in W, it follows that these conditions also hold for all $x, y, z \in W$.

- Verifying (VS 3): Since $W \neq \emptyset$, let $x \in W$. By the definition of subspaces, W is closed under scalar multiplication, $0x \in W$. But by Theorem 1.2(2), $0x$ is the zero vector of V, which we will denote by 0_V. Thus we have proved that $0_V \in W$. Since (VS 3) holds for V using 0_V as the zero vector, because W is a subset of V, and because $0_V \in W$, it follows that (VS 3) holds for W using 0_V as the zero vector for W.

- Verifying (VS 4): Let $x \in W$ and let $u = (-1)x$. By definition of subspaces, $u \in W$. Also, u is the additive inverse (in V) of x, by the last statement in Theorem 1.2(3) and Definition 5, so $x + u = 0_V$. Since 0_V is the zero vector for W as proved above, we have shown that u is an additive inverse for x in W. Thus (VS 4) holds for elements in W. □

Note: If you are reading Friedberg et al.'s textbook, then you will notice that the conclusion of our Theorem 1.3 is Friedberg et al's *definition* of the term subspace. Our definition of subspace is the condition appearing in Friedberg et al's Theorem 1.3 (subspace test). Luckily, their definition and ours are equivalent to each other. In this course you should use our definition as "the" definition.

Example 8.

1. Let V be a vector space. Then $\{0\}$ and V are always subspaces of V.
2. $\mathrm{P}_2(\mathbb{R})$ (the set of all polynomials of degree at most 2 and with real coefficients; see Definition 4) is a subspace of $\mathbb{R}[x]$ (the vector space of *all* polynomials with real coefficients) because $\mathrm{P}_2(\mathbb{R})$ is a subset of $\mathbb{R}[x]$, $0 \in \mathrm{P}_2(\mathbb{R})$, and $\mathrm{P}_2(\mathbb{R})$ is closed under addition and scalar multiplication defined on $\mathbb{R}[x]$.
3. The set $W = \{(a_{ij}) \in M_{n\times n}(\mathbb{F}) \mid \sum_{k=1}^{n} a_{kk} = 0\}$ is a subspace of $M_{n\times n}(\mathbb{F})$.
4. The set $W = \{(a_{ij}) \in M_{n\times n}(\mathbb{F}) \mid \sum_{k=1}^{n} a_{kk} = 1\}$ is not a subspace of $M_{n\times n}(\mathbb{F})$.

Remark 4. To check condition (S 1) in the definition of subspaces, we normally check whether $0 \in W$ or not.

Recall that the notion of a **subspace** of a vector space was defined in the previous week's lecture notes. Here are some facts about subspaces of some specific vector spaces, to help you build some intuition. We will not prove these facts now, but they will follow from theorems which will be proved during the next several weeks.

Example 9.

1. Subspaces of $\mathbb{R}^2$ are easily described. They are $\mathbb{R}^2$, $\{0\}$ (here 0 represents the origin $(0,0)$), and all lines in $\mathbb{R}^2$ which pass through the origin.

2. Subspaces of $\mathbb{R}^3$ are also easily described. They are $\mathbb{R}^3$, $\{0\}$ where 0 now represents $(0,0,0)$, all lines in $\mathbb{R}^3$ through the origin, and all planes in $\mathbb{R}^3$ through the origin.

3. Note that every plane in $\mathbb{R}^3$ through the origin can be defined by a single linear equation of the form $ax + by + cz = 0$. Any line in $\mathbb{R}^3$ through the origin can be described as the set of all scalar multiples of any one particular (nonzero) vector in the line.

4. More generally, if $\mathbb{F}$ is any field, then:

   (a) The subspaces of $\mathbb{F}^2$ are $\mathbb{F}^2$, $\{0\}$, and all "lines" in $\mathbb{F}^2$ through 0, where a "line in $\mathbb{F}^n$ through 0" is the set of all scalar multiples of a given nonzero vector in $\mathbb{F}^n$.

   (b) The subspaces of $\mathbb{F}^3$ are $\mathbb{F}^3$, $\{0\}$, all lines in $\mathbb{F}^3$ through 0, and all "planes" in $\mathbb{F}^3$ through 0 (which are subsets of $\mathbb{F}^3$ defined by a linear equation of the form $ax + by + cz = 0$ where $a, b, c \in \mathbb{F}$ with a, b, c not all 0).

   You might want to think about what this means if $\mathbb{F}$ is $\mathbb{C}$ or $\mathbb{Z}_5$.

5. Subspaces of $\mathbb{R}^4, \mathbb{R}^5$, etc. are somewhat more complicated to describe. But we will be able to describe them all, and it turns out that each subspace will have a definite "dimension." The same is true of subspaces of $\mathbb{F}^4, \mathbb{F}^5$, etc. for any field $\mathbb{F}$.

6. And then there are subspaces of vector spaces V where V does *not* have the form $\mathbb{F}^n$ for any field $\mathbb{F}$ and integer n. Though we cannot literally picture these vector spaces or their subspaces, we can imagine that their subspaces of "dimension 1" are "lines" (through 0), their subspaces of "dimension 2" are "planes" (through 0), and their subspaces of "dimension" higher than 2 are some higher-dimensional analogue of lines and planes. The theory of dimension will be developed in weeks 3 and 4.

1.4 Linear Combinations and Systems of Linear Equations

Definition 7. *Let V be a vector space over $\mathbb{F}$ and S a nonempty subset of V. A vector $x \in V$ is called a linear combination of vectors of S if there exist a* **finite number** *of vectors $u_1, \ldots, u_n \in S$ and scalars $a_1, \ldots, a_n \in \mathbb{F}$ such that*

$$x = a_1 u_1 + \cdots + a_n u_n.$$

Note that n must be strictly positive in the above equation, and $n = 1$ is allowed.

We also say that x is a linear combination of $u_1, \ldots, u_n$ and call $a_1, \ldots, a_n$ the coefficients of the linear combination.

Define $\operatorname{span}(S)$ to be the ***set*** *of all linear combinations of vectors in S.*

For convenience, we also define the span of the empty set to be $\operatorname{span}(\varnothing) = \{0\}$.

Example 10.

1. In $\mathbb{R}^3$, the span of $(1,0,0)$ and $(0,1,0)$ is the set

   $$\{a(1,0,0) + b(0,1,0) \,:\, a, b \in \mathbb{R}\}$$

   which can be written more simply as

   $$\{(a,b,0) \,:\, a, b \in \mathbb{R}\}.$$

   We might recognize that this set is just the x,y-plane in $\mathbb{R}^3$ (defined by the equation $z = 0$).

2. Recall that $\mathbb{Q}[x]$ is the vector space of all polynomials in x with rational coefficients. If S is the infinite subset $\{x, x^2, x^3, \ldots, x^n, \ldots\}$, what is $\operatorname{span}(S)$?

   Answer: It turns out that $\operatorname{span}(S)$ is the set of all polynomials in $\mathbb{Q}[x]$ whose constant coefficient equals 0 (exercise).

3. Suppose V is a vector space over $\mathbb{F}$ and $S \subseteq V$. It is easy to see that if S is a finite set of vectors, say $S = \{v_1, \ldots, v_n\}$, then the span of S is the span of $v_1, \ldots, v_n$, i.e.,

   $$\operatorname{span}(S) = \{a_1 v_1 + \cdots + a_n v_n \,:\, a_1, \ldots, a_n \in \mathbb{F}\}.$$

   (This is not completely trivial; for example, if R denotes the right-hand side of the above equation, then vectors of the form $a_1 v_1$ are in $\operatorname{span}(S)$ since they are linear combinations of finitely many vectors in S, but are they in R? Well, we can also see that $a_1 v_1 = a_1 v_1 + 0 v_2 + \cdots + 0 v_n$ which puts $a_1 v_1 \in R$ as claimed.)

   Next suppose that S is a countably infinite set of vectors $S = \{v_1, v_2, \ldots, v_n, \ldots\}$. Then we can use similar tricks to argue that

   $$\operatorname{span}(S) = \operatorname{span}(\{v_1\}) \cup \operatorname{span}(\{v_1, v_2\}) \cup \operatorname{span}(\{v_1, v_2, v_3\}) \cup \cdots \cup \operatorname{span}(\{v_1, \ldots, v_n\}) \cup \cdots$$

   (Exercise: prove both inclusions.)

   If S is uncountable (yes, nothing prevents this case), then there are no obvious simplifications available; $\operatorname{span}(S)$ is simply the set of all possible linear combinations of finitely many vectors from S.

Now we will illustrate a connection between linear combinations and systems of linear equations via the following example.

Example 11. Consider the vector space $M_{2\times 2}(\mathbb{R})$ of 2×2 matrices over $\mathbb{R}$. Determine whether $\begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}$ is a linear combination of

$$\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}.$$

Solution. For $\begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}$ to be a linear combination of the other three matrices, there needs to exist scalars (real numbers in this example) a, b, c satisfying

$$a \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} + c \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}.$$

We can write this more simply as

$$\begin{bmatrix} a & 0 \\ -a & 0 \end{bmatrix} + \begin{bmatrix} 0 & b \\ b & b \end{bmatrix} + \begin{bmatrix} c & c \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}$$

and even more simply as

$$\begin{bmatrix} a+c & b+c \\ -a+b & b \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}.$$

Since matrices are equal if and only if their corresponding entries are equal, this last equation simplifies to the following system of four linear equations:

$$\begin{cases} a & & & + & c & = & 1 \\ & + & b & + & c & = & 2 \\ -a & + & b & & & = & -3 \\ & & b & & & = & 4. \end{cases}$$

The point of this example is that the original question (is the first matrix in the span of the other three matrices?) turns out to be equivalent to asking whether the above system of 4 linear equations in the three unknowns a, b, c has a solution in real numbers (remember that in this example, the scalars are real numbers). We can easily solve the above system: since $b = 4$ (by the 4th equation), we get $a = 7$ (from the 3rd equation) and $c = -2$ (by the 2nd equation). But these values fail to satisfy the first equation. Hence the system of linear equations has no solution, so the matrix $\begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}$ is **not** a linear combination of the other three matrices. □

In this course, you are going to need to solve lots of small systems of linear equations over various fields, so what follows next is a brief explanation of how you should do that. (Much later in the course, you will learn more sophisticated techniques for solving systems of linear equations in any number of variables.)

Solving systems of linear equations by elimination

Here is an example of a system of 3 linear equations in 4 variables ranging over $\mathbb{R}$:

$$\begin{aligned} a_1 &+ 2a_2 - a_3 + a_4 = 5 \\ a_1 &+ 4a_2 - 3a_3 - 3a_4 = 6 \\ 2a_1 &+ 3a_2 - a_3 + 4a_4 = 8 \end{aligned}$$

$a_1, \ldots, a_4$ are the **variables**. (Could be $x_1, \ldots, x_4$, or anything else.)

Does this system have a solution (in $\mathbb{R}$)?

We answer this by **simplifying the system** via step-by-step elimination of variables.

Step 1: eliminate two occurrences of a_1.

1. Add -1 times the 1st equation to the 2nd equation. The new system is

$$\begin{aligned} a_1 &+ 2a_2 - a_3 + a_4 = 5 \\ &\quad 2a_2 - 2a_3 - 4a_4 = 1 \\ 2a_1 &+ 3a_2 - a_3 + 4a_4 = 8 \end{aligned}$$

   Claim: the new system has the same solutions as the original system.

   Proof. Not hard to see that no solutions are lost by this simplification. Conversely, we can retrieve the original system by adding the 1st equation to the (new) 2nd equation, so by the same logic, any solution to the new system is also a solution to the original. □

2. Add -2 times the 1st equation to the 3rd equation. The new system is

$$\begin{aligned} a_1 &+ 2a_2 - a_3 + a_4 = 5 \\ &\quad 2a_2 - 2a_3 - 4a_4 = 1 \\ &\quad -a_2 + a_3 + 2a_4 = -2 \end{aligned}$$

Step 2: Eliminate all but one occurrence of a_2.

3. Add 2 times the 3rd equation to the 1st equation. The new system is

$$\begin{aligned} a_1 &+ a_3 + 5a_4 = 1 \\ 2a_2 &- 2a_3 - 4a_4 = 1 \\ -a_2 &+ a_3 + 2a_4 = -2 \end{aligned}$$

4. Add 2 times the 3rd equation to the 2nd equation. The new system is

$$\begin{aligned} a_1 &+ a_3 + 5a_4 = 1 \\ &\quad 0 = -3 \\ -a_2 &+ a_3 + 2a_4 = -2 \end{aligned}$$

Remark 5. The second equation is a contradiction, so the original system has *no solutions*.

Suppose we change this example slightly: replace the "4" in the 3rd (original) equation with "3." Running through the above steps, this time at the end of Step 2 we get

$$\begin{aligned} a_1 \quad + \quad a_3 \quad + \quad 3a_4 &= 1 \\ -2a_4 &= -3 \\ -a_2 \quad + \quad a_3 \quad + \quad a_4 &= -2 \end{aligned}$$

Step 3: Eliminate all but one occurrence of a_4. [Why not a_3? Technically, that would be OK too. Later in the course we will develop an algorithm which in effect only eliminates variables that at occur as the "first" variable of an equation, as a_4 does here, so I will eliminate a_4 instead of a_3.]

5. Add 3/2 times the 2nd equation to the 1st equation. The new system is

$$\begin{aligned} a_1 \quad + \quad a_3 &= -7/2 \\ -2a_4 &= -3 \\ -a_2 \quad + \quad a_3 \quad + \quad a_4 &= -2 \end{aligned}$$

6. Add 1/2 times the 2nd equation to the 3rd equation. The new system is

$$\begin{aligned} a_1 \quad + \quad a_3 &= -7/2 \\ -2a_4 &= -3 \\ -a_2 \quad + \quad a_3 &= -7/2 \end{aligned}$$

You might think at this point that we should next try to eliminate one of the two occurrences of a_3. But doing so will either introduce a new occurrence of a_1 to the third equation, or a new occurrence of a_2 to the first equation. We don't want to do that, because we have already eliminated occurrences of a_1 and a_2. So we stop, having failed to find a contradiction.

In this situation, solutions are guaranteed to exist. To see it:

Step 4: Clean up

7. Multiply the 2nd equation by $-1/2$ and the 3rd equation by -1. The new system is

$$\begin{aligned} a_1 \quad + \quad a_3 &= -7/2 \\ a_4 &= 3/2 \\ a_2 \quad - \quad a_3 &= 7/2 \end{aligned}$$

8. Swap the 2nd and 3rd equations. The new system is

$$\begin{aligned} a_1 \quad + \quad a_3 &= -7/2 \\ a_2 \quad - \quad a_3 &= 7/2 \\ a_4 &= 3/2 \end{aligned}$$

This system is "fully simplified." If we replace a_3 with a parameter t in the first two equations, move these occurrences of t to the right-hand side, and add the equation $a_3 = t$, then we can read off the

solutions:

$$\begin{aligned} a_1 &= -t - 7/2 \\ a_2 &= t + 7/2 \\ a_3 &= t \\ a_4 &= 3/2 \end{aligned}$$

Here t is a **parameter**; it can be any real number. For each value of $t \in \mathbb{R}$, the above formulas give a solution to the original system. For example, $(a_1, a_2, a_3, a_4) = (-7/2, 7/2, 0, 3/2)$ is one solution (when $t = 0$). Another is $(a_1, a_2, a_3, a_4) = (-7, 7, 7/2, 3/2)$ (when $t = 7/2$).

Afraid that you might have made an arithmetical mistake? You can always substitute the above formulas for a_1, a_2, a_3, a_4 into the original equations and check that they work out.

The method of elimination can be used to solve systems of linear equations over any field. In general, the "allowed simplifications" of this method are:

- Add a scalar multiple of one equation to another equation.
- Multiply an equation by a **nonzero** scalar.
- Swap two equations.

Only eliminate all occurrences (but one) of a variable once.

If an equation of the form $0 = c$ is obtained where $c \neq 0$, then **no solutions**.

(If an equation of the form $0 = 0$ is found, you can delete it.)

If no contradiction is found, then replace the variables not eliminated by parameters, move the parameters to the right-hand side, and add dummy equations $a_i =$ (parameter for a_i) for them. The resulting equations should describe all solutions to the original system.

We now return to the general discussion of linear combinations and span. The most important fact to know about spans is that the span of a set is always a subspace of the ambient vector space.

Theorem 1.4. *Let S be a subset of a vector space V. Then* $\text{span}(S)$ *is a subspace of V. Moreover,* $\text{span}(S)$ *is the smallest subspace of V which contains S, in the sense that:*

1. $\text{span}(S)$ ***is*** *a subspace of V containing S, and*
2. *If W is any* ***other*** *subspace of V containing S, then $W \supseteq \text{span}(S)$.*

Proof Sketch. Consider the cases $S = \emptyset$ and $S \neq \emptyset$ separately.

- Use the definitions of $\text{span}(S)$ and of subspaces to verify $\text{span}(S)$ is a subspace of V.
- Verify $S \subseteq \text{span}(S)$.
- Let W be a subspace that contains S. Prove that $\text{span}(S) \subseteq W$.

Full details will be given in the recorded modules. □

Definition 8. *Let V be a vector space and S a subset of V. We say that S generates (or spans) V if* $\text{span}(S) = V$.

Remark 6. Let V be a vector space and S a subset of V. Since $\text{span}(S)$ is a subset of V, so to prove $\text{span}(S) = V$, it is sufficient to prove that every vector in V can be written as a linear combination of vectors in S.

Example 12. Show that the vectors $(1,0,0), (0,1,1), (1,0,1)$ generate $\mathbb{F}^3$, where $\mathbb{F}$ is a given field.

Proof. I won't reveal how I know this (can you figure it out?), but the following logic is air-tight: given any vector $(a,b,c) \in \mathbb{F}^3$, first note that since $a, b, c \in F$, then $a+b-c$ and $c-b$ are also elements of $\mathbb{F}$ (no matter what field $\mathbb{F}$ is). Now you can check that

$$(a+b-c)(1,0,0) + b(0,1,1) + (c-b)(1,0,1) = (a,b,c).$$

So I've written (a,b,c) as a linear combination of $(1,0,0)$, $(0,1,1)$, $(1,0,1)$. Since (a,b,c) was arbitrary, this shows that every vector in $\mathbb{F}^3$ can be written as a linear combination of the three given vectors. □

Example 13. In $\mathbb{F}^n$, denote e_j the vector whose j-th coordinate is 1 and whose other coordinates are 0. Prove that $\{e_1, \ldots, e_n\}$ generates $\mathbb{F}^n$.

Proof. In the recorded modules. □

Quick questions: Let $S = \{x_1, \ldots, x_k\}$ be a spanning set for a vector space V.

1. If we add an additional vector x_{k+1} to the set S, will we still have a spanning set? Explain.
2. If we delete one of the vectors, say x_k, from the set S, will we still have a spanning set? Explain.
3. Let U be the subspace of $\mathbb{R}^2$ spanned by e_1 and let W be the subspace of $\mathbb{R}^2$ spanned by e_2. Is $U \bigcup W$ a subspace of $\mathbb{R}^2$. Explain.

1.5 Linear Dependence and Linear Independence

Definition 9. *Let V be a vector space and S be a subset of V.*

- *The set S is called linearly dependent if there exist a* **finite number** *of* **distinct** *vectors $u_1, \ldots, u_n$ in S and scalars $c_1, \ldots, c_n$,* **not all zero**, *such that*

$$c_1 u_1 + \cdots + c_n u_n = 0.$$

  In this case, we also say that the vectors of S are linearly dependent. Note that n must be strictly positive in the above equation, and $n = 1$ is allowed.

- *The set S is called linearly independent if S is not linearly dependent. That is, for every choice of* **distinct** *$u_1, \ldots, u_n \in S$ with $n \geq 1$, whenever $c_1, \ldots, c_n \in \mathbb{F}$ are scalars satisfying*

$$c_1 u_1 + \cdots + c_n u_n = 0,$$

  then $c_i = 0$, for all $i = 1, \ldots n$.
  In this case, we also say that the vectors of S are linearly independent.

Remark 7.

1. For any vectors $u_1, \ldots, u_n$ in V, we always have the following representation of $0 \in V$ as a linear combination of $u_1, \ldots u_n$:

$$0u_1 + \cdots + 0u_n = 0,$$

   (all coefficients are 0). This is called the trivial representation of 0 as a linear combination of $u_1, \ldots u_n$.

2. The empty set is linearly independent since linear dependent sets must be nonempty by definition.

3. The set $S = \{0\}$ is linear dependent since $1 \cdot 0 = 0$ is a nontrivial representation of 0 as a linear combination of finitely many distinct vectors (i.e., the one vector) in S.

4. When S is a finite nonempty set, $S = \{u_1, \ldots, u_n\}$, where care has been taken to list the elements of S without repeats, then the definitions of linear independence and linear dependence can be simplified as follows:

   - $\{u_1, \ldots, u_n\}$ is linearly dependent iff there exist $(c_1, \ldots, c_n) \in \mathbb{F}^n$, $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$ with

$$c_1 u_1 + \cdots + c_n u_n = 0.$$

     In other words, the equation witnessing linear dependence can be assumed to mention all of the vectors in S.

   - $\{u_1, \ldots, u_n\}$ is linearly independent iff the following condition is satisfied:
     Whenever $c_1, \ldots, c_n \in \mathbb{F}$ are such that

$$c_1 u_1 + \cdots + c_n u_n = 0,$$

     then $c_i = 0$ for all $i = 1, \ldots, n$. In other words, the definition of linear independence only needs to be checked for linear combinations involving all of the vectors in S.

5. Any subset of a vector space that contains the zero vector is linearly dependent (exercise).

Example 14. Is $S = \{(0,1,1),(1,0,1),(1,2,3)\}$ linearly dependent in $\mathbb{R}^3$?
SOLUTION. We search for scalars $a, b, c \in \mathbb{R}$, not all 0, satisfying

$$a\begin{pmatrix}0\\1\\1\end{pmatrix} + b\begin{pmatrix}1\\0\\1\end{pmatrix} + c\begin{pmatrix}1\\2\\3\end{pmatrix} = \begin{pmatrix}0\\0\\0\end{pmatrix}.$$

The left-hand side is $\begin{pmatrix} b+c \\ a+2c \\ a+b+3c \end{pmatrix}$, so we need to solve the system

$$\begin{array}{rcrcrcl} & & b & + & c & = & 0 \\ a & & & + & 2c & = & 0 \\ a & + & b & + & 3c & = & 0. \end{array}$$

Elimination and simplification produces

$$\begin{array}{rcrcrcl} a & & & + & 2c & = & 0 \\ & & b & + & c & = & 0 \end{array} \qquad \text{and so} \qquad \begin{array}{rcl} a & = & -2c \\ b & = & -c \\ c & = & c \end{array}$$

For example, $(a,b,c) = (2,1,-1)$ is a solution in which not all of a, b, c are 0. Thus S is linearly dependent.

Example 15. Is the set $\{1, x, x^2, x^3\}$ linearly independent in $\mathbb{Z}_5[x]$?
SOLUTION. We look for scalars $a_0, a_1, a_2, a_3 \in \mathbb{Z}_5$ satisfying $a_0 1 + a_1 x + a_2 x^2 + a_3 x^3 = 0$ (the zero polynomial). By definition, a polynomial is the zero polynomial iff all of its coefficients are 0. So the only solution is

$$a_0 = a_1 = a_2 = a_3 = 0,$$

which proves that $\{1, x, x^2, x^3\}$ is linearly independent in $\mathbb{Z}_5[x]$. (Note that this proof had nothing to do with $\mathbb{Z}_5$, or with the power 3; the same proof shows that $\{1, x, x^2, \ldots, x^n\}$ is a linearly independent subset of $\mathbb{F}[x]$ for any field $\mathbb{F}$ and any positive integer n.)

Example 16. Let $\mathbb{F}$ be a field. The set $\{1, x, x^2, \ldots, x^n, \ldots\}$ of all powers of x is a linearly independent subset of $\mathbb{F}[x]$. For if we take any finite number of *distinct* powers $x^{k_1}, x^{k_2}, \ldots, x^{k_n}$ from S, then the only scalars $a_1, \ldots, a_n \in \mathbb{F}$ which can make $a_1 x^{k_1} + \cdots + a_n x^{k_n}$ equal to the zero polynomial is the trivial choice $a_1 = \cdots = a_n = 0$.

The word "dependent" is used because when vectors are linearly dependent, then (at least) one of them "depends on" the others. The following theorem makes this precise.

Theorem 1.5. *Let S be a subset of a vector space V. Then S is linearly dependent if and only either $S = \{0\}$ or some vector in S is a linear combination of other vectors in S.*

Proof. Let $\mathbb{F}$ be the field of scalars for V.

($\Leftarrow$) We have already explained why $\{0\}$ is linearly dependent. Suppose the vector $v \in S$ can be written as a linear combination of *other* vectors $u_1, \ldots, u_n \in S$, say

$$v = c_1u_1 + \cdots + c_nu_n, \qquad c_1, \ldots, c_n \in \mathbb{F}.$$

We can assume with no loss of generality that $u_1, \ldots, u_n$ are distinct. Since $v \notin \{u_1, \ldots, u_n\}$ by assumption, it follows that $u_1, \ldots, u_n, v$ are distinct. Now note that $(-1)v = -v$ by Theorem 1.2(3) and so

$$c_1u_1 + \cdots + c_nu_n + (-1)v = 0.$$

As $u_1, \ldots, u_n, v$ are distinct vectors in S and at least one of the coefficients (-1) in the above linear combination is not 0, we get that S is linearly dependent.

($\Rightarrow$) Assume S is linearly dependent. Thus there exist distinct $u_1, \ldots, u_n \in S$ and $a_1, \ldots, a_n \in \mathbb{F}$, not all 0, such that $a_1u_1 + \cdots + a_nu_n = 0$. By "weeding out" terms a_iu_i where $a_i = 0$, we can assume that $a_i \neq 0$ for all $i = 1, \ldots, n$.

Case 1: $n = 1$. Then $a_1u_1 = 0$ with $a_1 \neq 0$. This implies $u_1 = 0$ (exercise, using (VS 5) and (VS 6) and property (F 4) of fields), so $0 \in S$. If $S = \{0\}$ then we're done. Assume $S \neq \{0\}$. Then we can pick $v \in S \setminus \{0\}$, and we can write $0 = 0v$, proving that some vector (0) in S can be written as a linear combination of another vector (v) of S.

Case 2: $n > 1$.

Then since $a_n \neq 0$, we can solve for u_n and express it as a linear combination of $u_1, \ldots, u_{n-1}$. In more detail (this is the last time we will give such detail): Adding $-(a_nu_n)$ to both sides of $a_1u_1 + \cdots + a_nu_n = 0$ gives

$$(a_1u_1 + \cdots + a_{n-1}u_{n-1} + a_nu_n) + -(a_nu_n) = 0 + -(a_nu_n).$$

Associating and applying (VS 1), (VS 3) and (VS 4) gives

$$a_1u_1 + \cdots + a_{n-1}u_{n-1} = -(a_nu_n).$$

Multiplying both sides by -1 and applying A1Q2(a) and Theorem 1.2(3) gives

$$(-a_1)u_1 + \cdots + (-a_{n-1})u_{n-1} = a_nu_n.$$

Now multiply both sides by a_n^{-1} (recall that $a_n \neq 0$) and apply A1Q2(a) and (VS 5) and (VS 6) to get

$$u_n = (-a_n^{-1}a_1)u_1 + \cdots + (-a_n^{-1}a_{n-1})u_{n-1}.$$

Hence u_n can be expressed as a linear combination of other elements in S. $\square$

1.6 Bases and Dimension

Definition 10. *Let V be a vector space. A subset S of V is called a basis for V if it satisfies the following two conditions:*

1. *S is linearly independent.*
2. *S spans V.*

If S is a basis for V, we also say that the vectors of S form a basis for V.

Next, for each of the popular vector spaces in this course, we will give an example of a basis for that vector space.

Example 17.

1. The empty set is a basis for the zero vector space since the empty set spans $\{0\}$ and is a linear independent subset of $\{0\}$.
2. In $\mathbb{F}^n$, consider the subset $S = \{e_1, \ldots, e_n\}$, where $e_j \in \mathbb{F}^n$ is the vector whose j-th coordinate is 1 and whose other coordinates are 0. In Week 02, Example 13, we prove that S spans $\mathbb{F}^n$. On the other hand, if
$$c_1 e_1 + \ldots + c_n e_n = 0,$$
for some scalars $c_1, \ldots, c_n \in \mathbb{F}$, then
$$(c_1, \ldots, c_n) = 0.$$
Therefore, $c_1 = \ldots = c_n = 0$, which means S is linear independent. In conclusion, S is a basis for $\mathbb{F}^n$. We call S the standard basis for $\mathbb{F}^n$.
3. In $M_{m\times n}(\mathbb{F})$, the set $\{E_{ij} \in M_{m\times n}(\mathbb{F}) : 1 \le i \le m, 1 \le j \le n\}$ is a basis for $M_{m\times n}(\mathbb{F})$. Here E_{ij} is an $m \times n$ matrix, where the entry at i-th row, j-th column is 1 and the remaining entries are 0. Proof is left as an exercise.
4. In $P_n(\mathbb{F})$, the set $S = \{1, x, \ldots, x^n\}$ is a basis for $P_n(\mathbb{F})$, called the standard basis for $P_n(\mathbb{F})$. Proof is left as an exercise.
5. In $\mathbb{F}[x]$, the set $S = \{1, x, x^2, \ldots\}$ is a basis. Proof is left as an exercise.

The following theorem states an important property of a basis for a vector space.

Theorem 1.6. *Let $\{v_1, \ldots, v_n\}$ be a basis for a vector space V. Then every $x \in V$ can be* **uniquely expressed** *as a linear combination of $v_1, \ldots, v_n$. That is, there is a unique n-tuple, $(a_1, \ldots, a_n) \in \mathbb{F}^n$ such that*
$$x = a_1 v_1 + \ldots + a_n v_n.$$

Proof.

- Existence: Since $\{v_1, \ldots, v_n\}$ is a basis of V, the set $\{v_1, \ldots, v_n\}$ generates V. Therefore, there exist scalars $a_1, \ldots, a_n \in \mathbb{F}$ such that $x = a_1 v_1 + \ldots + a_n v_n$.
- Uniqueness: Suppose there are also $b_1, \ldots, b_n \in \mathbb{F}$ such that

$$x = a_1 v_1 + \cdots + a_n v_n = b_1 v_1 + \cdots + b_n v_n.$$

$$(a_1 - b_1)v_1 + \cdots + (a_n - b_n)v_n = 0.$$

Since $\{v_1, \ldots, v_n\}$ is linearly independent, $a_1 - b_1 = \ldots = a_n - b_n = 0$. So $a_k = b_k$ for all $k = 1, \ldots, n$.

□

Comments:

- Given an arbitrary vector space V, it is natural to ask the following questions about bases:
  1. Does V have a basis?
  2. If a basis for V exists, can we find at least one basis for V?
  3. Can a vector space have more than one basis?
- We will first answer the first two questions. One potential approach is to first build a linear independent subset in V and keep adding vectors to the linear independent set so that the new set is still linearly independent. When that process ends, we get the "largest" linearly independent subset (in the sense that adding any new vector to that largest linearly independent set, the new set becomes linearly dependent). Finally, we will prove that largest linear independent subset also spans V. Rigorously, we need to make sure that the adding process will eventually ends. Before discussing the existence theorem, let us recall some notations about sets.

Definition 11.

- *A set is countably infinite if there is a 1-1 mapping between the set and* $\mathbb{N}$*. For example,* $\mathbb{Z}$ *and* $\mathbb{Q}$ *are countably infinite.*
- *A set is countable if it is a finite set or it is countably infinite.*
- *A set is uncountable if it is not countable. For example,* $\mathbb{R}, \mathbb{C}$*, and* $(0, 1)$ *are uncountable.*

The following theorem shows the existence of a basis and indicate how to find a basis of countably spanned vector spaces.

Theorem 1.7. *If a vector space* V *is generated by a countable set* S*, then some subset of* S *is a basis for* V*.*

Proof Sketch. If $S = \emptyset$ or $S = \{0\}$, then $V = \{0\}$ and $\emptyset$ is a subset of S that is a basis for V. Otherwise, S contains at least a nonzero vector. Since S is countable,

$$S = \{v_1, \ldots, v_n\} \quad \text{or} \quad S = \{v_1, v_2, \ldots, \}.$$

Denote $i_1 \geq 1$ the smallest index such that $v_{i_1} \neq 0$. Note v_{i_1} exists since S contains a nonzero vector. Then $\{v_{i_1}\}$ is linearly independent.
Let i_2 be the smallest index such that $v_{i_2} \in S$ and $v_{i_2} \notin \text{span}(\{v_{i_1}\})$. Continuing this process, take $v_{i_k} \in S$ such that $v_{i_k} \notin \text{span}(\{v_{i_1}, \ldots, v_{i_{k-1}}\})$, $k \geq 2$.
Denote $T = \{v_{i_k} \in S \mid v_{i_k} \notin \text{span}(\{v_{i_1}, \ldots, v_{i_{k-1}}\}, k \geq 1\}$. An example of finding the set T from a given spanning set is presented in the recorded module, Wk03-mod3-ExistenceOfBases-part1.

We will prove that T is a basis for V.

- Prove that T is linearly independent by contradiction. Assume T is linearly dependent. Then there exist $a_1, \ldots, a_k$ not all zeros so that

$$a_1 v_{i_1} + \cdots + a_k v_{i_k} = 0.$$

  By removing the term $a_j v_{i_j}$ for $j = k, k-1, \ldots$ if $a_j = 0$, we can assume $a_k \neq 0$. Then we can write v_{i_k} as a linear combination of $v_{i_1}, \ldots, v_{i_{k-1}}$:

$$v_{i_k} = -a_k^{-1} a_1 v_{i_1} - \cdots - a_k^{-1} a_{k-1} v_{i_{k-1}},$$

  which contradicts the construction of v_{i_j} for $j \geq 1$.

- Prove that T spans V. In order to do that, we will first show by induction (see the recorded module, Wk03-mod4-ExistenceOfBases-part2) that $\text{span}(S_k) = \text{span}(T_k)$, where

$$S_k = \{v_1, \ldots, v_k\} \quad \text{and} \quad T_k = T \cap S_k = \{v_{i_q} \mid i_q \leq k\}.$$

  Now, we will prove $V = \text{span}(T)$. Let $x \in V = \text{span}(S)$. Then $x \in \text{span}(S_m)$ for m large enough. So $x \in \text{span}(T_m) \subset \text{span}(T)$. Therefore, $V = \text{span}(T)$.

□

Indeed, we can prove the existence of a basis for any vector space.

Theorem 1.8. *Every vector space has a basis.*

The detailed proof can be found in Section 1.7 (Friedberg et al.'s textbook) using maximal linearly independent subsets and Zorn's lemma (optional reading).

The next main result is to prove that any two bases of a finitely spanned vector space have the same number of elements, which leads to the notation of dimensions of vector spaces. To prove this, we first have an intermediate result.

Theorem 1.9 (Replacement Theorem)**.** *Suppose V is a vector space with a finite spanning set S. Let T be a linearly independent subset in V. Then*

1. *$|T| \leq |S|$.*
2. *There exists a set $H \subseteq S$ containing exactlly $(|S| - |T|)$ vectors such that $T \cup H$ generates V.*

Proof. Denote $n = |S|$. We will prove the theorem by induction on the size of the linearly independent set, $m = |T|$.

- Base case: When $m = 0$, clearly $m = 0 \leq |S|$.
- Assume the statement is true for some $m \geq 0$. That is, if T_m is any linearly independent subset in V of size m, then $m \leq n$ and there exists a set $H_m \subseteq S$ containing exactly $n - m$ vectors such that $T_m \cup H_m$ generates V.
- Let $T = \{v_1, \ldots, v_{m+1}\}$ be a linearly independent subset of V. We need to prove that $m + 1 \leq n$ and there exists a subset H of S of exactly $n - m - 1$ vectors so that $T \cup H$ spans V.

  Let $T_m = \{v_1, \ldots, v_m\}$. Since T_m is a subset of T and T is linearly independent, T_m is also linear independent.

  Applying the induction hypothesis on T_m, we have $n \geq m$ and there exist $(n - m)$ vectors $w_{m+1}, \ldots, w_n$ in S such that $\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n\}$ generates V.

  Since $n \geq m$, either $n = m$ or $n > m$. If $n = m$, the spanning set of V, $\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n\}$ becomes $\{v_1, \ldots, v_m\}$. Therefore, $v_{m+1} \in V = \text{span}\{v_1, \ldots v_m\}$. By Theorem 1.5, the set $T = \{v_1, \ldots, v_m, v_{m+1}\}$ is linearly dependent, a contradiction. Therefore, $n \neq m$. Combining with $n \geq m$, we obtain $n > m$. Hence $n \geq m + 1$.

  For the second part of the statement, the idea here is to replace a vector from the spanning set $\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n\}$ by v_{m+1}. To begin with, we can write v_{m+1} as a linear combination of the spanning set $\{v_1, \ldots, v_m, w_{m+1}, \ldots, w_n\}$:

  $$v_{m+1} = a_1 v_1 + \ldots + a_m v_m + a_{m+1} w_{m+1} + \ldots + a_n w_n, \tag{1}$$

  for some scalars $a_1, \ldots, a_n \in \mathbb{F}$.

  Claim: At least one of the scalars $a_{m+1}, \ldots, a_n$ is nonzero. Indeed, if $a_{m+1} = \ldots = a_n = 0$, then Equation (1) becomes

  $$v_{m+1} = a_1 v_1 + \ldots + a_m v_m.$$

  Therefore, the set T is linearly dependent, a contradiction. This completes the proof of the claim.

  Go back to the main theorem, since at least one of the scalars $a_{m+1}, \ldots, a_n$ is nonzero, without loss of generality, we assume that $a_{m+1} \neq 0$. From Equation (1), we have

  $$\begin{aligned} a_{m+1} w_{m+1} &= -a_1 v_1 - \ldots - a_m v_m + v_{m+1} - a_{m+2} w_{m+2} - \ldots - a_n w_n \\ w_{m+1} &= -a_{m+1}^{-1} a_1 v_1 - \ldots - a_{m+1}^{-1} a_m v_m + a_{m+1}^{-1} v_{m+1} - a_{m+1}^{-1} a_{m+2} w_{m+2} - \ldots - a_{m+1}^{-1} a_n w_n. \end{aligned}$$

  Denote $H = \{w_{m+2}, \ldots, w_n\} \subset S$. We have shown that $w_{m+1} \in \text{span}(T \cup H)$.

  In addition, $v_1, \ldots, v_m \in T \subset T \cup H$ and $w_{m+2}, \ldots, w_n \in H \subset T \cup H$. Therefore,

  $$V = \text{span}\{w_{m+1}, v_1, \ldots, v_m, w_{m+2}, \ldots, w_n\} \subset \text{span}(T \cup H).$$

  Clearly, $\text{span}(T \cup H) \subset V$. Therefore, $V = \text{span}(T \cup H)$, which completes the proof of the theorem.

□

Corollary 1.9.1. Suppose V is a finitely spanned vector space. Then all bases of V are finite and have the same number of elements.

Proof. Let S be a finite spanning set for V. Let B be a basis for V. Then B is linearly independent. By the Replacement theorem, $|B| \leq |S| < \infty$.

Now, let B_1 and B_2 be two bases for V. Since B_1 is linearly independent and B_2 is a finite spanning set for V, by the Replacement theorem, we have $|B_1| \leq |B_2|$. Similarly, since B_2 is linearly independent and B_1 is a finite spanning set for V, by the Replacement theorem, we have $|B_2| \leq |B_1|$. Therefore, $|B_1| = |B_2|$. □

Definition 12.

- *A vector space is called finite-dimensional if it has a basis consisting of a finite number of vectors.*
- *Let V be a finite dimensional vector space. The unique number of vectors in each basis for V is called the dimension of V and is denoted by $\dim V$.*
- *Convention:* $\dim\{0\} = 0$.
- *A vector space that is not finite-dimensional is called infinite dimensional.*

To find the dimension of a vector space, one can find a basis for that vector space and count the number of elements in that basis.

Example 18.

1. Since $\{e_1, \ldots, e_n\} \subset \mathbb{F}^n$ is a basis for F^n, we conclude $\dim \mathbb{F}^n = n$.
2. $\dim_{\mathbb{R}} \mathbb{R}^n = n$, $\dim_{\mathbb{C}} \mathbb{C}^n = n$, $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$, where $\dim_{\mathbb{R}} \mathbb{C}^n$ means the dimension of the vector space $\mathbb{C}^n$ over the field of real numbers and $\dim_{\mathbb{C}} \mathbb{C}^n$ means the dimension of the vector space $\mathbb{C}^n$ over the field of complex numbers.

   Proof Sketch. Applying part 1 for $\mathbb{F} = \mathbb{R}$ and $\mathbb{F} = \mathbb{C}$, we have $\dim_{\mathbb{R}} \mathbb{R}^n = n$, $\dim_{\mathbb{C}} \mathbb{C}^n = n$.

   For the vector space $\mathbb{C}^n$ over the field of real numbers, we can verify (exercise) that the following set is a basis for $\mathbb{C}^n$ over the field $\mathbb{R}$:

   $$S = \{e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1), \omega_1 = (i, 0, \ldots, 0), \ldots, \omega_n = (0, \ldots, 0, i)\}.$$

   □
3. Similarly, we have $\dim M_{m\times n}(\mathbb{F}) = mn$ since the set $S = \{E_{ij} : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for $M_{m\times n}(\mathbb{F})$, where E_{ij} is an $m \times n$ matrix whose entry at row ith, column jth is one and whose other entries are zero.
4. Similarly, $\dim P_n(\mathbb{F}) = n + 1$ since the set $\{1, x, \ldots, x^n\}$ is a basis for $P_n(\mathbb{F})$.

Next, we will present some other corollaries of the Replacement Theorem.

Corollary 1.9.2. Let V be a vector space with dimension n.

1. Any finite spanning set for V contains at least n vectors.
2. A generating set for V that contains exactly n vectors is a basis for V.
3. Any linearly independent subset of V has at most n vectors.
4. Any linearly independent subset of V that contains exactly n vectors is a basis for V.
5. Every linearly independent subset of V can be extended to a basis for V.
6. Let W be a subspace of V. Then $\dim W \leq \dim V$. The equality happens if and only if $W = V$.
7. Let W be a subspace of V. Then any basis for W can be extended to a basis for V.

Proof. Let β be a basis for V.

(1 &2) Let S be a finite spanning set for V. By the Existence Theorem (Theorem 1.7), some subset T of S is a basis for V. Therefore, $|T| = \dim V = n$. Also, since T is a subset of S, $|S| \geq |T|$. Therefore, $|S| \geq n$. Moreover, if $|S| = n$, $|S| = |T|$. Since $T \subseteq S$, S must equal to T. That means S is a basis for V.

(3) Applying the replacement theorem for the spanning set β, the size of any linearly independent subset of V is at most the size of the spanning set β. Therefore, any linearly independent subset of V has at most $|\beta| = n$ vectors

(4) Suppose T is a linearly independent subset of V that contains exactly n vectors. Applying the Replacement theorem for the spanning set β and the linearly independent set T, there is a subset H of β containing $|\beta| - |T| = n - n = 0$ vectors such that $T \cup H$ generates V. Since $|H| = 0$, $H = \emptyset$ and $T \cup H = T$. Therefore, the set T spans V. Since T is also linearly independent, T is a basis for V.

(5) Let $L = \{v_1, \ldots, v_k\}$ be a linearly independent subset in V. If $k = n$, by part 4, we conclude that L is a basis for V.

If $k < n$, applying the Replacement theorem for the spanning set β and the linearly independent set L, there is a subset H of β containing $|\beta| - |L| = n - k$ vectors such that $L \cup H$ generates V. By part 1, $|L \cup H| \geq n$. On the other hand, we have

$$|L \cup H| = |L| + |H| - |L \cap H| = k + n - k - |L \cap H| = n - |L \cap H| \leq n.$$

Therefore, $|L \cup H| = n$. By part 2, $L \cup H$ is a basis for V.

(6) Case 1: $W = \{0\}$, them $\dim W = 0 \leq \dim V$.
Case 2: W has a nonzero vector w_1.

- The set $\{w_1\}$ is linearly independent.
- Continuing choosing the vectors $w_1, w_2, \ldots, w_k$ in W such that $\{w_1, \ldots, w_k\}$ is linearly independent.
- Note that $\{w_1, \ldots, w_k\}$ is also a linearly independent subset of V so we cannot go on indefinitely linearly independent elements of W. Suppose this process stops at stage $k \leq n$ where $T = \{w_1, \ldots, w_k\}$ is a linearly independent subset of W and adding any other vectors from W to the set T will produce a linearly dependent set.
- By Theorem 1.5 (week 02 lecture notes), $W \subset \text{span}(T)$. Since T is a subset of W, we have $\text{span}(T) \subset \text{span}(W) = W$. Therefore, $\text{span}(T) = W$. In conclusion the set T is linearly indepdent subset of W and spans W. Therefore, T is a basis for W and

$$\dim W = |T| = k \leq n = \dim V.$$

- If $\dim V = \dim W = n$, then a basis for W is a linearly independent set containing n elements. By Corollary 1.9.2 part 4, that set is also a basis for V.

(7) By part 6, $\dim W \leq \dim V$. Let $\{w_1, \ldots, w_k\}$ be a basis for W. Then $\{w_1, \ldots, w_k\}$ is a linearly independent subset in W, which is also a linearly independent subset in V. By part 5, we can extend that linearly independent subset to a basis for V.

□

Week 4. Quotient Spaces. Sum and Direct Sum of Subspaces.

1.7 Quotient Spaces

To construct a vector space, we need a set, 2 operations, and 8 conditions. We have encountered vector spaces V where elements are n-tuples, matrices, polynomials, functions. Today, we will study a vector space where each element is a set.

Throughout this section, we denote V a vector space over $\mathbb{F}$ and W a subspace of V.

Definition 13.

- *For each $x \in V$, we define $x + W$ the following subset of V:*

$$x + W = \{x + w \mid w \in W\}.$$

The set $x + W$ is called a coset of W in V and x is called a representative of the coset $x + W$.

- *For $x, y \in V$, if $x - y \in W$, we write $x \equiv y \pmod{W}$.*
- *Denote V/W (pronounced "V mod W") the collection of cosets of W in V:*

$$V/W = \{x + W \mid x \in V\}.$$

Example 19.

1. Consider a vector space V and W a subspace of V. Then

$$0 + W = \{0 + w \mid w \in W\} = \{w \mid w \in W\} = W.$$

2. Consider a vector space V and $W = \{0\}$. Then for any $x \in V$, $x + W = \{x\}$. Also, $V/\{0\} = \{\{x\} : x \in V\}$. We consider $V/\{0\} = V$.

3. Consider $V = \mathbb{R}^3$, $W = \{(a, 2a, 3a) \mid a \in \mathbb{R}\}$ a subspace of V, and $x = (1, -1, 4) \in V$. Then

$$x + W = \{x + w \mid w \in W\} = \{(1, -1, 4) + (a, 2a, 3a) \mid a \in \mathbb{R}\} = \{(a + 1, 2a - 1, 3a + 4) \mid a \in \mathbb{R}\}.$$

Therefore, $x + W$ is a line going through $(1, -1, 4)$ and parallels to the line W. The set V/W is a collection of lines in $\mathbb{R}^3$ that parallel to W.

Proposition 1. *Let W be a subspace of a vector space V and $x, y \in V$.*

1. *$x \in x + W$.*
2. *$x + W = y + W$ if and only if $x - y \in W$. In particular, $x + W = W$ if and only if $x \in W$.*

Proof. In the recorded module. □

Remark 8.

1. The relation $\equiv \pmod{W}$ is an equivalence relation on V. That is, $\equiv \pmod{W}$ is reflexive, symmetric, and transitive. (See the proof in the recorded module).
2. For the first round of reading, it'd better to stick with the definition V/W as the collection of cosets of W in V. The visualization of the set V/W is not always easy to see.

Original domain	$\mathbb{Z}$	Vector space V
Modding by	m	subspace W
Equivalence relation	$\equiv \pmod{m}$	$\equiv \pmod{W}$
Equivalence class	$[k]$	x+W
Set of equivalence class	$\mathbb{Z}_m$	V/W

Table 1: The analogy between the constructions of $\mathbb{Z}_m$ and V/W

3. The construction of V/W is analogous to the construction of $\mathbb{Z}_m$ (see Table 1).

Next, we will define the operations on V/W to make V/W a vector space.

Definition 14. *Let V be a vector space over $\mathbb{F}$ and W be a subspace of V. Operations of addition and scalar multiplication by $\mathbb{F}$ are defined naturally on V/W by representatives:*

$$(x+W)+(y+W) := x+y+W,$$

$$a(x+W) := ax+W,$$

for any $a \in \mathbb{F}$ and $x, y \in V$.

Lemma 1. *Under the assumptions in Definition 14, the two operations are well-defined. It means, for elements in V/W,*

1. *If $x_1+W = x_2+W$ and $y_1+W = y_2+W$, then $(x_1+W)+(y_1+W) = (x_2+W)+(y_2+W)$.*
2. *If $x_1+W = x_2+W$, then $a(x_1+W) = a(x_2+W)$, for any $a \in \mathbb{F}$.*

Proof. 1. Since $x_1+W = x_2+W$, by Proposition 1, $x_2-x_1 \in W$. Since $y_1+W = y_2+W$, by Proposition 1, $y_2-y_1 \in W$. So $(x_2+y_2)-(x_1+y_1) = (x_2-x_1)+(y_2-y_1) \in W$. Again, by proposition 1, $x_1+y_1+W = x_2+y_2+W$. So $(x_1+W)+(y_1+W) = (x_2+W)+(y_2+W)$.

2. Exercise. □

Example 20. Returning to Example 19 part 2, addition of two lines $x+W$ and $y+W$ in V/W is the line $x+y+W \in V/W$ going through the point $(x+y) \in V$ and paralleling to the line W. The scalar multiplication of a line $x+W \in V/W$ by a scalar $a \in \mathbb{F}$ is the line $ax+W$ going through the point $ax \in V$ and paralleling to the line W.

Theorem 1.10. *The set V/W with the two operations defined in Definition 14 is a vector space over $\mathbb{F}$. The vector space V/W is called the quotient space of V by W.*

Proof Sketch. . Verify all 8 conditions of vector spaces. The zero vector of V/W is W. □

For every vector space, we first want to know its dimension and identify a basis for that vector space. For the quotient space V/W, we have the following result.

Theorem 1.11. *Let V be a finite dimensional vector space and W be a subspace of V. Let $\{v_1, \ldots, v_n\}$ be a basis for V such that $\{v_1, \ldots, v_k\}$ is a basis for W $(k \leq n)$. Then*

1. *The set* $\{v_{k+1} + W, \ldots, v_n + W\}$ *is a basis for* V/W.

2. $\dim(V/W) = \dim V - \dim W$.

Proof Sketch. 1. We will prove the set $\{v_{k+1}+W, \ldots, v_n+W\}$ is linearly independent (using Proposition 1 and the assumption that $\{v_1, \ldots, v_k\}$ is a basis for W) and generates V/W (using the assumption that $\{v_1, \ldots, v_n\}$ is a basis for V). See the detailed proof in the recorded module.

2. By part 1, $\dim(V/W) = n - k = \dim V - \dim W$. Therefore, $\dim V = \dim W + \dim(V/W)$.

□

For example, with $V = \mathbb{R}^3$ and $W = \{(a, 2a, 3a) \mid a \in \mathbb{R}\}$ is a line through the origin, then $\dim(\mathbb{R}^3/W) = \dim \mathbb{R}^3 - \dim W = 2$.

Remark 9. There are also cases where both V and W are infinite dimensional, but $\dim(V/W)$ is finite. For example, $V = \mathbb{F}^\infty$ and $W = \{(0, x_2, x_3, \ldots) \mid x_k \in \mathbb{F}\}$. Note that any element of V/W is just determined by the value of the first coordinate x_1. We can verify that $\dim(V/W) = 1$ (see recorded modules).

1.8 Sums and Internal Direct Sums of Subspaces

Definition 15. *Let* V *be a vector space over* $\mathbb{F}$ *and* W_1, W_2 *be subspaces of* V.

- *Define the sum of the subspaces* W_1 *and* W_2 *as follows:*

$$W_1 + W_2 := \{v_1 + v_2 \mid v_1 \in W_1, v_2 \in W_2\}.$$

- *If in addition,* $W_1 \cap W_2 = \{0\}$*, we say* W_1 *and* W_2 *are independent, or disjoint, and we write* $W_1 \oplus W_2$ *for* $W_1 + W_2$*. The set* $W_1 \oplus W_2$ *is also called the (internal) direct sum of the subspaces* W_1 *and* W_2.

- *If* $W_1 \oplus W_2 = V$ *(i.e.,* $W_1 + W_2 = V$ *and* $W_1 \cap W_2 = \{0\}$*), then* W_2 *is called a a complementary subspace to* W_1.

Remark 10. Let V be a vector space over $\mathbb{F}$ and W_1, W_2 be subspaces of V. Then the direct sum of W_1 and W_2, $W_1 \oplus W_2$, is defined whenever $W_1 \cap W_2 = \{0\}$.

Lemma 2. *Let* V *be a vector space over* $\mathbb{F}$ *and* W_1, W_2 *be subspaces of* V*. Then*

1. $W_1 \cap W_2$ *is a subspace of* W_1*,* W_2*, and* V.

2. $W_1 + W_2$ *is the smallest subspace of* V *containing* W_1 *and* W_2.

3. $V = W_1 \oplus W_2$ *if and only if for every vector* v *in* V*, there exist unique element* $w_1 \in W_1$ *and* $w_2 \in W_2$ *so that* $v = w_1 + w_2$.

Proof. 1. Exercise.

2. First, we will prove that $W_1 + W_2$ is a subspace of V. By definition of subspaces, it is sufficient to prove that $W_1 + W_2$ is closed under addition and scalar multiplication. Let $(v_1 + v_2), (u_1 + u_2) \in W_1 + W_2, a \in \mathbb{F}$, where $v_1, u_1 \in W_1$ and $v_2, u_2 \in W_2$. Since W_1 and W_2 are subspaces of $W_1 + W_2$, $v_1 + u_1 \in W_1$, $v_2 + u_2 \in W_2$, $av_1 \in W_1$, and $av_2 \in W_2$. Therefore,

$$(v_1 + v_2) + (u_1 + u_2) = (v_1 + u_1) + (v_2 + u_2) \in W_1 + W_2,$$

$$a(v_1 + v_2) = av_1 + av_2 \in W_1 + W_2,$$

which implies $W_1 + W_2$ is a subspace of V.

Also, for every vector v_1 in W_1, we have $v_1 = v_1 + 0 \in W_1 + W_2$. Therefore, $W_1 \subset W_1 + W_2$. Similarly, $W_2 \subset W_1 + W_2$.

Finally, let Y be a subspace of V that contains both W_1 and W_2. Since Y is closed under addition, every addition $v_1 + v_2$, where $v_1 \in W_1, v_2 \in W_2$, is an element in Y. Therefore, $W_1 + W_2 \subset Y$. In conclusion, $W_1 + W_2$ is the smallest subspace of V that contains W_1 and W_2.

3. ($\Rightarrow$) Since $V = W_1 \oplus W_2$, $V = W_1 + W_2$ and $W_1 \cap W_2 = \{0\}$. Let $v \in V$. Since $V = W_1 + W_2$, $v \in W_1 + W_2$. By the definition of $W_1 + W_2$, there exist $w_1 \in W_1$ and $w_2 \in W_2$ so that $v = w_1 + w_2$.

Suppose we also have $v = w_1' + w_2'$ for some $w_1' \in W_1, w_2' \in W_2$. Then

$$0 = (w_1 + w_2) - (w_1' + w_2') = (w_1 - w_1') + (w_2 - w_2')$$

$$w_1 - w_1' = w_2' - w_2.$$

Since $w_1, w_1' \in W_1$, $w_1 - w_1' \in W_1$. Since $w_2, w_2' \in W_2$, $w_2' - w_2 \in W_2$. Therefore,

$$w_1 - w_1' = w_2' - w_2 \in W_1 \cap W_2 = \{0\}.$$

Hence $w_1 - w_1' = w_2' - w_2 = 0, w_1 = w_1', w_2 = w_2'$, which proves the uniqueness of the representation.

($\Leftarrow$) Since every vector in V can be written as $w_1 + w_2$ for some $w_1 \in W_1$ and $w_2 \in W_2$, $V \subseteq W_1 + W_2$. By part 2, we also have $W_1 + W_2 \subseteq V$. Therefore, $V = W_1 + W_2$. It remains to prove that $W_1 \cap W_2 = \{0\}$. Let $x \in W_1 \cap W_2$. Then $-x \in W_1 \cap W_2$. We can write 0 as follows:

$$0 = 0 + 0 \in W_1 + W_2,$$

$$0 = x + (-x) \in W_1 + W_2.$$

Due to the uniqueness assumption, $x = 0$. Therefore, $W_1 \cap W_2 = \{0\}$. Hence $V = W_1 \oplus W_2$. □

In the following examples, we will describe the sum of two given subspaces.

Example 21. Let $V = \mathbb{R}^3$.

1. Let W_1 be the x-axis and W_2 be the y-axis:

$$W_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}, \quad W_2 = \{(0, y, 0) \mid y \in \mathbb{R}\}.$$

Then

$$W_1 + W_2 = \{(x, 0, 0) + (0, y, 0) \mid (x, 0, 0) \in W_1, (0, y, 0) \in W_2\} = \{(x, y, 0) \mid x, y \in \mathbb{R}\}.$$

Therefore, $W_1 + W_2$ is the xy-plane.

2. Let W_1 be the xy-plane and W_2 be the plane defined by $y - z = 0$:

$$W_1 = \{(x, y, 0) \mid x, y \in \mathbb{R}\}, \quad W_2 = \{(x, y, y) \mid x, y \in \mathbb{R}\}.$$

Intuitively, $W_1 + W_2$, the smallest subspace of $\mathbb{R}^3$ that contains both those planes, should be $\mathbb{R}^3$. Let's verify that intuition formally. We have

$$W_1 + W_2 = \{(x, y, 0) + (x, y, y) \mid x, y \in \mathbb{R}\} = \{(2x, 2y, y) \mid x, y \in \mathbb{R}\} = \{(x, y, z) \mid y - 2z = 0\},$$

which is not $\mathbb{R}^3$. What went wrong? Indeed, a correct calculation should be

$$W_1 + W_2 = \{(x, y, 0) + (x', y', y') \mid x, y, x', y' \in \mathbb{R}\} = \{(x + x', y + y', y') \mid x, y, x', y' \in \mathbb{R}\}.$$

This formulation is correct, although it is difficult to see geometrically why such expression leads to the conclusion that $W_1 + W_2 = \mathbb{R}^3$. Indeed, we can verify that $W_1 + W_2 = \mathbb{R}^3$ from the observation that every vector (x, y, z) in $\mathbb{R}^3$ can be written as:

$$(x, y, z) = (x, y - z, 0) + (0, z, z) \in W_1 + W_2.$$

Therefore, $\mathbb{R}^3 \subseteq W_1 + W_2$. Since $W_1 + W_2 \subseteq \mathbb{R}^3$ by definition, we conclude that $W_1 + W_2 = \mathbb{R}^3$.

Theorem 1.12. *Let V be a vector space over $\mathbb{F}$ and W_1, W_2 be two finite dimensional subspaces of V. Then*

1. *$W_1 + W_2$ is finite dimensional and*

$$\dim(W_1) + \dim(W_2) = \dim(W_1 + W_2) + \dim(W_1 \cap W_2).$$

2. *If V is finite dimensional and $W_1 \oplus W_2 = V$, then*

$$\dim W_1 + \dim W_2 = \dim V.$$

Proof. 1. To prove a dimension equality, a popular method is to construct a suitable basis for each subspace on both sides of the equality. Then by counting the number of elements in those bases, we obtain the conclusion. For this question, we start with a basis for $W_1 \cap W_2$. Note that $W_1 \cap W_2$ is a subspace of W_1 so $\dim(W_1 \cap W_2) \leq \dim W_1 < \infty$ (see Week 3 lectures, Corollary 1.9.2). Then we extend that basis of $W_1 \cap W_2$ to get a basis for W_1 and a basis for W_2. Note that we always can do such extensions (see Week 3 lectures, Corollary 1.9.2. Finally, we can select a basis for $W_1 + W_2$ from those vectors. Here is the detailed proof.

Since $W_1 \cap W_2$ is a subspace of W_1 and $\dim W_1 < \infty$, $\dim(W_1 \cap W_2) \leq \dim W_1 < \infty$. Suppose $\{u_1, \ldots, u_k\}$ is a basis for $W_1 \cap W_2$. Since $W_1 \cap W_2$ is a subspace of the finite dimensional vector space W_1, we can extend $\{u_1, \ldots, u_k\}$ to get a basis $S_1 = \{u_1, \ldots, u_k, v_1, \ldots, v_m\}$ for W_1. Similarly, since $W_1 \cap W_2$ is a subspace of the finite dimensional vector space W_2, we can extend $\{u_1, \ldots, u_k\}$ to get a basis $S_2 = \{u_1, \ldots, u_k, z_1, \ldots, z_p\}$ for W_2. We will prove that

$$S = \{u_1, \ldots, u_k, v_1, \ldots, v_m, z_1, \ldots, z_p\}$$

is a basis for $W_1 + W_2$.

- Verify that S is linearly independent. Consider

$$a_1u_1 + \cdots + a_ku_k + b_1v_1 + \cdots + b_mv_m + c_1z_1 + \cdots + c_pz_p = 0, \tag{2}$$

for some scalars $a_1, \ldots, a_k, b_1, \ldots, b_m, c_1, \ldots c_p$. Then

$$b_1v_1 + \cdots + b_mv_m = -a_1u_1 - \cdots - a_ku_k - c_1z_1 - \cdots - c_pz_p.$$

Since the right hand side of the above equation is a linear combination of vectors in W_2, the right hand side of the above equation is a vector in W_2. On the other hand, since the left hand side of the above equation is a linear combination of vectors in W_1, the left hand side of the above equation is in W_1. Therefore, $b_1v_1 + \cdots + b_mv_m \in W_1 \cap W_2$.

Since $\{u_1, \ldots, u_k\}$ is a basis for $W_1 \cap W_2$, there are scalars $d_1, \ldots, d_k$ so that

$$b_1v_1 + \cdots + b_mv_m = d_1u_1 + \cdots + d_ku_k.$$

So

$$b_1v_1 + \cdots + b_mv_m - d_1u_1 - \cdots - d_ku_k = 0.$$

Since $\{u_1, \ldots, u_k, v_1, \ldots, v_m\}$ is a basis for W_1,

$$b_1 = \ldots = b_m = d_1 = \ldots = d_k = 0.$$

Substituting $b_1 = ldots = b_m = 0$ to Equation (2), we have

$$a_1u_1 + \cdots + a_ku_k + c_1z_1 + \cdots + c_pz_p = 0.$$

Since $\{u_1, \ldots, u_k, z_1, \ldots, z_p\}$ is a basis for W_2, we have

$$a_1 = \ldots = a_k = c_1 = \cdots = c_p = 0.$$

Therefore, the set S is linearly independent.

- Verify that S generates $W_1 + W_2$. Let $x + y \in W_1 + W_2$, where $x \in W_1, y \in W_2$. Since S_1 and S_2 are bases for W_1 and W_2, respectively, we can write x and y as linear combinations of vectors in S_1 and S_2, respectively:

$$x = a_1u_1 + \cdots + a_ku_k + b_1v_1 + \cdots + b_mv_m,$$

$$y = d_1u_1 + \cdots + d_ku_k + c_1z_1 + \cdots + c_pz_p,$$

where $a_1, \ldots, a_k, b_1, \ldots, b_m, d_1, \ldots, d_k, c_1, \ldots, c_p \in \mathbb{F}$. Then

$$x + y = (a_1 + d_1)u_1 + \cdots + (a_k + d_k)u_k + b_1v_1 + \cdots + b_mv_m + c_1z_1 + \cdots + c_pz_p.$$

Therefore, $x + y \in \text{span}\,(S)$. So $W_1 + W_2 \subseteq \text{span}\,(S)$. On the other hand, since $S \subset W_1 + W_2$ and $W_1 + W_2$ is a vector space, $\text{span}\,(S) \subseteq W_1 + W_2$. Hence $W_1 + W_2 = \text{span}(S)$.

In conclusion, we have proved S is a basis for $W_1 + W_2$. Therefore,

$$\dim(W_1 + W_2) = |S| = m + p + k,$$

$$\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = m + p + k + k = (m + k) + (p + k) = \dim W_1 + \dim W_2.$$

2. Since $W_1 \oplus W_2 = V$, $W_1 \cap W_2 = \{0\}$ and $W_1 + W_2 = V$. Applying part 1, we have

$$\begin{aligned}\dim V &= \dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2 = \dim W_1 + \dim W_2 - \dim\{0\} \\ &= \dim W_1 + \dim W_2 - 0 = \dim W_1 + \dim W_2.\end{aligned}$$

□

Example 22. 1. Suppose W_1 is a 5-dimensional subspace of $\mathbb{R}^8$. If W_2 is a complementary subspace to W_1 then $\dim W_2 = 3$.

2. If W_1 is a 3-dimensional subspace of $\mathbb{R}[x]$, and W_2 is a complementary subspace of W_1, then W_2 must be infinite-dimensional. Indeed, if W_2 is finite dimensional, $\dim V = \dim W_1 + \dim W_2 < \infty$, a contradiction.

3. If $W_1 = \text{span}(\{1, x, x^2\})$ in $\mathbb{R}[x]$, then $W_2 = \text{span}(\{x^3, x^4, \ldots\})$ is a complementary subspace to W_1.

Remark 11. 1. **(Existence of Complementary Subspaces.)** In Assignment 3 and Week 3 lectures, we have proved that every finite linear independent set can be extended to a basis for a vector space V that has a countable spanning set. Indeed, every linearly independent subset of a vector space V can be extended to a basis for V (note that all assumptions about finite or countable sets are removed). Therefore, every subspace of a vector space V has a complementary subspace.

2. It's also good to know whether complementary subspaces of a given subspace is unique or not. The answer is NO. Can you find a counter example? That is, find W_1, W_2, U_2 subspaces of some vector space V so that $V = W_1 \oplus W_2 = W_1 \oplus U_2$ and $W_2 \neq U_2$.

2 Linear Transformations and Matrices

2.1 Linear Transformations, Null Spaces, and Ranges

Definition 16. *Let V and W be vector spaces over the same field $\mathbb{F}$. A function $T : V \to W$ is called a linear transformation from V to W, or is said to be linear if, for all $x, y \in V$ and $c \in \mathbb{F}$, we have*

(L1) $T(x + y) = T(x) + T(y)$ *and*

(L2) $T(cx) = cT(x)$.

Proposition 2. *Consider a mapping $T : V \to W$. Then T is linear iff $T(cx + y) = cT(x) + T(y)$ for all $x, y \in V$ and $c \in \mathbb{F}$.*

Proof. Exercise. □

Example 23. 1. Let V and W be vector spaces. The following functions are linear:

(a) $T_0 : V \to W$, $T_0(x) = 0$, for all $x \in V$. The function T_0 is called the zero transformation.

(b) $I_V : V \to V$, $I_V(x) = x$, for all $x \in V$. The function I_V is called the identity transformation on V.

2. Define $T : \mathbb{R}^2 \to \mathbb{R}^2$ by $T(x_1, x_2) = (x_1, -x_2)$. Claim: T is linear (T is called the reflection about the x-axis).

Proof. Let $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}^2$ and $c \in \mathbb{F}$. Then

$$\begin{aligned} T(cx + y) = T(c(x_1, x_2) + (y_1, y_2)) &= T((cx_1 + y_1, cx_2 + y_2)) = (cx_1 + y_1, -cx_2 - y_2) \\ = (cx_1, -cx_2) + (y_1, -y_2) &= c(x_1, -x_2) + (y_1, -y_2) = cT(x) + T(y). \end{aligned}$$

Therefore, T is linear. □

3. Let V be a finite dimensional vector space over $\mathbb{F}$ and let $\{v_1, \ldots, v_n\}$ be a basis for V. The following mapping is linear:

$$T : V \to \mathbb{F}^n, \quad T(a_1 v_1 + \cdots + a_n v_n) := (a_1, \ldots, a_n).$$

Proof. Exercise. □

4. Let $1 \leq k < n$, consider the projection mapping $T : \mathbb{F}^n \to \mathbb{F}^k$, $T(x_1, \ldots, x_n) := (x_1, \ldots, x_k)$. Then T is linear.

Proof. Exercise. □

5. Define $T : M_{m\times n}(\mathbb{F}) \to M_{n\times m}(\mathbb{F})$ by $T(A) = A^t$, where A^t is the transpose of A. Then T is a linear transformation. Recall: let $A \in M_{m\times n}(\mathbb{F})$. Define $A^t \in M_{n\times m}(\mathbb{F})$ as follows: $A^t_{ij} = A_{ji}$ for all $1 \le j \le m, 1 \le i \le n$. That is, rows of A are collumns of A^t and vice versa.

   Proof. Let $A, B \in M_{m\times n}(\mathbb{F})$ and $c \in \mathbb{F}$. For any $1 \le j \le m, 1 \le i \le n$, we have

   $$(cA + B)^t_{ij} \overset{\text{by def}}{=} (cA + B)_{ji} = (cA)_{ji} + B_{ji} = cA_{ji} + B_{ji} \overset{\text{by def}}{=} c(A^t)_{ij} + (B^t)_{ij} = (cA^t + B^t)_{ij}.$$

   Therefore, $(cA + B)^t = cA^t + B^t$, $T(cA + B) = cT(A) + T(B)$. Hence T is linear. □

6. Define $D_n : P_n(\mathbb{R}) \to P_n(\mathbb{R})$ by $D_n(f(x)) = f'(x)$, where $f'(x)$ denotes the derivative of $f(x)$. Then D_n is linear.

   Proof. Exercise. Note that we can rewrite D_n as

   $$D_n(a_0 + a_1x + \ldots + a_nx^n) = a_1 + 2a_2x + \ldots + na_nx^{n-1},$$

   for all scalars $a_0, \ldots, a_n$. □

Proposition 3. *Let $T : V \to W$ be linear. Then*

1. $T(0) = 0$.
2. $T(x - y) = T(x) - T(y), \quad \forall x, y \in V$.
3. $T(a_1x_1 + \cdot + a_nx_n) = a_1T(x_1) + \cdots + a_nT(x_n)$.

Proof. 1. We have

$$T(0) = T(0 + 0) = T(0) + T(0) \Rightarrow 0 = T(0) + T(0) - T(0) = T(0).$$

2. Let $x, y \in V$. We have

$$T(x - y) = T(x) + T(-y) = T(x) + (-1)T(y) = T(x) - T(y).$$

3. Prove (3) by induction. Exercise. □

The next theorem will show us how a linear transformation $T : V \to W$ is determined when we know its values on the vectors in a basis of V.

Theorem 2.1. *Let $\{v_1, \ldots, v_n\}$ be a basis for a vector space V, and let $\{w_1, \ldots, w_n\}$ be arbitrary elements of a vector space W. Then there exists a unique linear mapping $T : V \to W$ such that*

$$T(v_1) = w_1, \ldots, T(v_n) = w_n.$$

Proof. **Existence.** We will construct a mapping $T : V \to W$ satisfying

$$T(v_1) = w_1, \ldots, T(v_n) = w_n.$$

Let $v \in V$. Since $\{v_1, \ldots, v_n\}$ is a basis for V, there exist $a_1, \ldots, a_n \in \mathbb{F}$ such that

$$v = a_1 v_1 + \cdots + a_n v_n.$$

Define $T(v) = T(a_1 v_1 + \cdots + a_n v_n) := a_1 w_1 + \cdots + a_n w_n$. By the construction, for any $1 \leq k \leq n$, we have

$$T(v_k) = T(0v_1 + \cdots + 0v_{k-1} + 1v_k + 0v_{k+1} + \cdots 0v_n) = 0w_1 + \cdots + 0w_{k-1} + 1w_k + 0w_{k+1} + \cdots 0w_n = w_k.$$

Next, we will verify that T is linear (exercise).

Uniqueness. Suppose there is another linear mapping $L : V \to W$ satisfying

$$L(v_1) = w_1, \ldots, L(v_n) = w_n.$$

Take $v \in V$, $v = a_1 v_1 + \cdots + a_n v_n$ for some scalars $a_1, \ldots, a_n$. Then

$$\begin{aligned} L(v) = L(a_1 v_1 + \cdots + a_n v_n) &\overset{Prop.\ 3.3}{=} a_1 L(v_1) + \cdots + a_n L(v_n) = a_1 w_1 + \cdots + a_n w_n \\ &= a_1 T(v_1) + \cdots + a_n T(v_n) \overset{Prop.\ 3.3}{=} T(a_1 v_1 + \cdots + a_n v_n) = T(v). \end{aligned}$$

So $T(v) = L(v)$, for any $v \in V$. Therefore, $T = L$.

□

From the proof of Theorem 2.1, we have the following result.

Corollary 2.1.1. Let $\{v_1, \ldots, v_n\}$ be a basis for a vector space V and $\{w_1, \ldots, w_n\}$ be arbitrary elements of a vector space W. Let $T : V \to W$ be the unique linear mapping such that

$$T(v_1) = w_1, \ldots, T(v_n) = w_n.$$

Then for all $a_1, \ldots, a_n \in \mathbb{F}$, we have

$$T(a_1 v_1 + \cdots + a_n v_n) = a_1 w_1 + \cdots + a_n w_n.$$

Definition 17. *Let V and W be vector spaces, and let $T : V \to W$ be linear. Define the following sets:*

- *Null space (or kernel) of T: $N(T) := \{x \in V \mid T(x) = 0_W\}$.*
- *Range (or image) of T: $R(T) := \{T(x) \mid x \in V\}$.*

Theorem 2.2. *Let $T : V \to W$ be linear. Then $N(T)$ is a subspace of V and $R(T)$ is a subspace of W.*

Proof. Exercise. □

Example 24. Consider the differential operator $D_n : P_n(\mathbb{R}) \to P_n(\mathbb{R})$, $D_n(p(x)) = p'(x)$. Then

$$N(D_n) = \{p(x) \in P_n(\mathbb{R}) \mid p'(x) = 0\} = \{p(x) = c \mid c \in \mathbb{R}\} = \text{span}(\{1\}),$$

$$R(D_n) = \{p'(x) \mid p(x) \in P_n(\mathbb{R})\} = P_{n-1}(\mathbb{R}).$$

Also, $\dim N(D_n) = 1$, $\dim R(D_n) = n$ and $\dim N(D_n) + \dim R(D_n) = n + 1 = \dim P_n(\mathbb{R})$.

Theorem 2.3. *Let V and W be vector spaces, and let $T : V \to W$ be linear. If $\{v_1, \ldots, v_n\}$ is a basis for V, then $\{T(v_1), \ldots, T(v_n)\}$ generates $R(T)$.*

Proof. See the recorded module. □

Example 25. Find a basis for the null space and for the range of a linear transformation.(see the recorded module)

Definition 18. *Let $T : V \to W$ be linear. If $\dim(N(T)) < \infty$, define* nullity(T) $:= \dim(N(T))$. *If $\dim(R(T)) < \infty$, define* rank(T) $:= \dim(R(T))$.

Theorem 2.4 (Rank-Nullity Theorem)**.** *Let V and W be vector spaces and $T : \mathbb{V} \to \mathbb{W}$ be linear. If $\dim(V) < \infty$, then*

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

Proof Sketch. Since $N(T)$ is a subspace of V and $\dim(V) < \infty$, we have nullity$(T) \leq \dim(V) < \infty$. Suppose nullity$(T) = k$ and $\{v_1, \ldots, v_k\}$ is a basis for $N(T)$. Extending $\{v_1, \ldots, v_k\}$ to get a basis for V, $\{v_1, \ldots, v_n\}$.
Claim: $\{T(v_{k+1}), \ldots, T(v_n)\}$ is a basis for $R(T)$.

(i) Show that $\{T(v_{k+1}), \ldots, T(v_n)\}$ spans $R(T)$.

By Theorem 2.2, we have

$$R(T) = \text{span}\left(\{T(v_1), \ldots, T(v_k), T(v_{k+1}), \ldots, T(v_n\})\right.\text{.}$$

Since $\{v_1, \ldots, v_k\}$ is a basis for $N(T)$, $T(v_1) = \ldots = T(v_k) = 0$. Therefore,

$$R(T) = \text{span}\left(\{T(v_{k+1}), \ldots, T(v_n\})\right.\text{.}$$

(ii) Show that $\{T(v_{k+1}), \ldots, T(v_n)\}$ is linearly independent.

Consider

$$c_{k+1}T(v_{k+1}) + \cdots + c_nT(v_n) = 0, \quad \text{where } c_{k+1}, \ldots, c_n \in \mathbb{F}.$$
$$T(c_{k+1}v_{k+1} + \cdots + c_nv_n) = 0.$$

Therefore, $c_{k+1}v_{k+1} + \cdots + c_nv_n \in N(T)$. Since $\{v_1, \ldots, v_k\}$ is a basis for $N(T)$, there exist $d_1, \ldots, d_k \in \mathbb{F}$ so that

$$c_{k+1}v_{k+1} + \cdots + c_nv_n = d_1v_1 + \cdots + d_kv_k$$
$$-d_1v_1 - \cdots - d_kv_k + c_{k+1}v_{k+1} + \cdots + c_nv_n = 0.$$

Since $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ is a basis for $\mathbb{V}$, we have

$$d_1 = \ldots = d_k = c_{k+1} = \ldots = c_n = 0.$$

Therefore, $\{T(v_{k+1}), \ldots, T(v_n)\}$ is linearly independent.

Combining (i) and (ii), we have the conclusion.

□

Definition 19. *Let $T : V \to W$ be linear. Then*

- *T is called one-to-one if $T(x) = T(y)$ implies $x = y$, or equivalently, if $x \neq y$ implies $T(x) \neq T(y)$.*
- *T is called onto if $R(T) = W$.*
- *T is called an isomorphism if T is one-to-one and onto.*

Lemma 3. *Let $T : V \to W$ be linear. Then T is one-to-one if and only if $N(T) = \{0\}$.*

Proof. ($\Rightarrow$) Suppose T is one-to-one. Let $x \in N(T)$. Then $T(x) = 0$. Since $T(0) = 0$ and T is one-to-one, $x = 0$. Therefore, $N(T) = \{0\}$.

($\Leftarrow$) Suppose $N(T) = \{0\}$. Consider $x, y \in V$ such that $T(x) = T(y)$. Then

$$0 = T(x) - T(y) = T(x - y).$$

Therefore $x - y \in N(T)$. Since $N(T) = \{0\}$, $x - y = 0$, $x = y$. Therefore, T is one-to-one. □

Theorem 2.5. *Let W be a vector spaces over a field $\mathbb{F}$ and let V be a finite-dimensional vector space over $\mathbb{F}$ and $\{v_1, \ldots, v_n\}$ be a basis for V. Consider a linear transformation $T : V \to W$. Then T is an isomorphism if and only if $\{T(v_1), \ldots, T(v_n)\}$ is a basis for W.*

Proof. ($\Rightarrow$) Suppose T is an isomorphism. We will prove that $\{T(v_1), \ldots, T(v_n)\}$ is linearly independent and generates W.

Consider $c_1T(v_1) + \cdots + c_nT(v_n) = 0$, where $c_1, \ldots, c_n \in \mathbb{F}$. So

$$T(c_1v_1 + \ldots + c_nv_n) = 0.$$

Since T is one-to-one, $c_1v_1 + \ldots + c_nv_n = 0$. Since $\{v_1, \ldots, v_n\}$ is a basis for V, we have $c_1 = \ldots = c_n = 0$. Therefore, $\{T(v_1), \ldots, T(v_n)\}$ is linearly independent.

Since T is an isomorphism, T is onto. Therefore, $W = R(T)$. By Theorem 2.3, $\{T(v_1), \ldots, T(v_n)\}$ generates $R(T)$. Hence $\{T(v_1), \ldots, T(v_n)\}$ generates W, which completes the proof.

($\Leftarrow$) Suppose $\{T(v_1), \ldots, T(v_n)\}$ is a basis for W. Then $\{T(v_1), \ldots, T(v_n)\}$ generates W, Therefore,

$$W = \text{span}(\{T(v_1), \ldots, T(v_n)\}) = R(T),$$

where the second equality comes from Theorem 2.3. Since $R(T) = W$, T is onto.

Let $x \in N(T)$. Since $\{v_1, \ldots, v_n\}$ is a basis for V, $x = a_1v_1 + \ldots + a_nv_n$, for some $a_1, \ldots, a_n \in \mathbb{F}$. So

$$0 = T(x) = T(a_1v_1 + \ldots + a_nv_n) = a_1T(v_1) + \ldots + a_nT(v_n).$$

Since $\{T(v_1), \ldots, T(v_n)\}$ is a basis for W, $\{T(v_1), \ldots, T(v_n)\}$ is linearly independent. Hence

$$a_1 = \ldots = a_n = 0,\ x = a_1v_1 + \ldots + a_nv_n = 0v_1 + \ldots + 0v_n = 0.$$

Thus $N(T) = \{0\}$. Therefore, T is one-to-one. □

Remark. From Theorem 2.5, to construct an isomorphism (if exists) between two finite-dimensional vector spaces, we choose a basis $\{v_1, \ldots, v_n\}$ for V and a basis $\{w_1, \ldots, w_n\}$ for W. Then define a linear transformation $T : V \to W$ such that $T(v_k) = w_k, \forall 1 \leq k \leq n$. By Theorem 2.1, such linear transformation exists. By Theorem 2.5, T is an isomorphism.

Example 26. Construct an isomorphism between two vector spaces. See the recorded module.

Definition 20. *Let V and W be two vector spaces over a field $\mathbb{F}$. The vector space V is said to be isomorphic to the vector space W if there is an isomorphism $T : V \to W$. Denote $V \cong W$.*

Theorem 2.6. *Let V and W be two finite-dimennsional vector spaces over a field $\mathbb{F}$. Then V is isomorphic to W if and only if $\dim V = \dim W$.*

Proof. See the recorded module. □

Example 27.

1. $P_n(\mathbb{F}) \cong \mathbb{F}^{n+1}$ since $\dim P_n(\mathbb{F}) = \dim \mathbb{F}^{n+1} = n + 1$.
2. $M_{m\times n}(\mathbb{F}) \cong \mathbb{F}^{mn}$ since $\dim M_{m\times n}(\mathbb{F}) = \dim \mathbb{F}^{mn}$.

Theorem 2.7. *Let V and W be two vector spaces over a field $\mathbb{F}$ of equal finite dimension. Let $T : V \to W$ be linear. Then the following statements are equivalent:*

1. *T is one-to-one.*
2. *T is onto.*
3. *$\operatorname{rank} T = \dim V$.*

Proof Sketch. Using the Rank-Nullity theorem. See the recorded module for the detailed proof □

Questions:

1. Let V and W be vector spaces over a field $\mathbb{F}$ and $T : V \to W$ be linear. Suppose $v_1, \ldots, v_n$ be vectors in a vector space V such that $\{T(v_1), \ldots, T(v_n)\}$ spans W. Prove that $\dim V \geq \dim W$.
2. Let $T : V \to U$ and $L : U \to W$ be linear mappings between finitely dimensional vector spaces V, U and W. Prove that
   (a) $\operatorname{rank}(L \circ T) \leq \min\{\operatorname{rank}(T), \operatorname{rank}(L)\}$
   (b) Compare $\operatorname{nullity}(L \circ T)$ with $\operatorname{nullity}(T)$ and $\operatorname{nullity}(L)$.

Definition 21. *Let V and W be vector spaces over $\mathbb{F}$. We let $\mathcal{L}(V,W)$ denote the set of* all *linear transformations $T : V \to W$.*

In particular, if $W = \mathbb{F}$ then $\mathcal{L}(V,\mathbb{F})$ is the subset of the vector space $\mathbb{F}^V$ consisting of those functions $T : V \to \mathbb{F}$ which are linear. It will follow from Theorem 2.8 (below) that $\mathcal{L}(V,\mathbb{F})$ is actually a sub*space* of $\mathbb{F}^V$.

More generally, if W is a vector space over $\mathbb{F}$ and D is any nonempty set, we can turn the set W^D of all functions from D to W into a vector space over $\mathbb{F}$, in the same way that we turned $\mathbb{F}^D$ into a vector space in Example 4. Namely, for functions $f, g \in W^D$ and scalar $c \in \mathbb{F}$ we define $f + g \in W^D$ and $cf \in W^D$ by

$$(f+g)(x) := f(x) + g(x) \quad \text{and} \quad (cf)(x) := cf(x), \quad x \in D,$$

where the addition and scalar multiplication on the right-hand sides of these two definitions are calculated in W. We will leave it to the reader to check that W^D is a vector space over $\mathbb{F}$.

Now assume as before that V, W are vector spaces over $\mathbb{F}$. Then $\mathcal{L}(V,W)$ is a subset of the vector space W^V of all functions from V to W.

Theorem 2.8. *Let V and W be vector spaces over $\mathbb{F}$. Then $\mathcal{L}(V,W)$ is a subspace of W^V.*

Proof. We already know that $\mathcal{L}(V,W)$ is a subset of W^V, so we only need to show that it is nonempty and is closed under the addition and scalar multiplication operations of W^V. Recall from Example 23 that we have the zero transformation $T_0 : V \to W$. Thus $\mathcal{L}(V,W)$ is nonempty. Next, assume that $T, U \in \mathcal{L}(V,W)$, i.e., T and U are linear transformations from V to W. We must show that $T+U \in \mathcal{L}(V,W)$, i.e., that $T+U$ is linear. Using Proposition 2, we check whether $(T+U)(cx+y) = c((T+U)(x)) + (T+U)(y)$ for all $x, y \in V$ and $c \in \mathbb{F}$. Well,

$$\begin{aligned}
(T+U)(cx+y) &= T(cx+y) + U(cx+y) && \text{(definition of the function } T+U) \\
&= (cT(x) + T(y)) + (cU(x) + U(y)) && \text{(as } T \text{ and } U \text{ are linear)} \\
&= (c(T(x) + U(x))) + (T(y) + U(y)) && \text{(calculating in the vector space } W) \\
&= c((T+U)(x)) + (T+U)(y) && \text{(definition of the function } T+U).
\end{aligned}$$

Hence $T+U$ is a linear transformation by Proposition 2, proving $T+U \in \mathcal{L}(V,W)$. A similar argument shows that $\mathcal{L}(V,W)$ is closed under scalar multiplication. □

Since we now know that $\mathcal{L}(V,W)$ is a vector space, we can ask questions like "What is its dimension?" We will answer this question in full generality in section 2.3. Before doing that, we will consider the specific case of $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$ and show a connection to matrices.

Definition 22. Matrix-Vector Multiplication: *Let $A \in M_{m\times n}(\mathbb{F})$ and $\mathbf{x} \in \mathbb{F}^n$. We consider $\mathbf{x}$ as an $n \times 1$* ***column vector*** $\mathbf{x} = (x_1, \ldots, x_n)^T = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$*. Then $A\mathbf{x}$ is the $m \times 1$ column vector in $\mathbb{F}^m$*

defined as follows:

$$A\mathbf{x} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^{n} a_{1k}x_k \\ \sum_{k=1}^{n} a_{2k}x_k \\ \vdots \\ \sum_{k=1}^{n} a_{mk}x_k \end{bmatrix}.$$

This looks more complicated than it actually is. Simply note that the ith entry of $A\mathbf{x}$ is obtained by multiplying the entries in the ith row of A by the entries of $\mathbf{x}$ and then summing up the products.

Example 28. Let $A = \begin{bmatrix} 2 & -1 & 0 \\ 3 & 4 & 1 \end{bmatrix} \in M_{2\times 3}(\mathbb{R})$. Then for any $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \in \mathbb{R}^3$ we have

$$\begin{bmatrix} 2 & -1 & 0 \\ 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2x_1 + (-1)x_2 + 0x_3 \\ 3x_1 + 4x_2 + 1x_3 \end{bmatrix} = \begin{bmatrix} 2x_1 - x_2 \\ 3x_1 + 4x_2 + x_3 \end{bmatrix}.$$

So for example,

$$\begin{bmatrix} 2 & -1 & 0 \\ 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ -7 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} 2 & -1 & 0 \\ 3 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ -10 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Definition 23. *If $\mathbb{F}$ is a field and $A \in M_{m\times n}(\mathbb{F})$, then L_A denotes the function $\mathbb{F}^n \to \mathbb{F}^m$ given by $L_A(\mathbf{x}) = A\mathbf{x}$.*

Example 28 (continued). With $A \in M_{2\times 3}(\mathbb{R})$ as in the example above, L_A is a function $\mathbb{R}^3 \to \mathbb{R}^2$. For example, $L_A((1, 1, -7)) = (1, 0)$ and $L_A((1, 2, -10)) = (0, 1)$.

Our next goal is to prove that each function L_A is a linear transformation. Here is a result that will help us do that.

Some matrix notations. Let $A \in M_{m\times n}(\mathbb{F})$.

- Recall that we use a_{ij} to denote the entry of A in the ith row and jth column. Thus $a_{ij} \in \mathbb{F}$.
- We often use a_j to denote the jth column of A. Thus $a_j \in \mathbb{F}^m$, and

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mj} & \cdots & a_{mn} \end{bmatrix} \qquad \text{and} \qquad a_j = \begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{ij} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

- We also write $A = [a_1 \;\; a_2 \;\; \cdots \;\; a_n]$ when $a_1, \dots, a_n \in \mathbb{F}^m$ are the columns of A.

Lemma 4. *Suppose $A \in M_{m\times n}(\mathbb{F})$ and write $A = [a_1 \;\; a_2 \;\; \cdots \;\; a_n]$, so $a_1, \ldots, a_n \in \mathbb{F}^m$ are the columns of A.*

1. *For any $\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{F}^n$ we have*

$$A\mathbf{x} = x_1a_1 + x_2a_2 + \cdots + x_na_n.$$

   That is, $A\mathbf{x}$ is the linear combination of the columns of A whose coefficients are the entries in $\mathbf{x}$.

2. *If $e_1, \ldots, e_n$ are the standard basis vectors for $\mathbb{F}^n$, then Ae_j equals the j-th column of A.*

Proof. In the recorded modules. □

Corollary 2.8.1 (Matrix Equality Theorem)**.** Let $A, B \in M_{m\times n}(\mathbb{F})$. Then $A = B$ if and only if $A\mathbf{x} = B\mathbf{x}$, for all $\mathbf{x} \in \mathbb{F}^n$.

Proof. $\Rightarrow$ is obvious. $\Leftarrow$ If $A\mathbf{x} = B\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}^n$, then in particular $Ae_j = Be_j$ for $j = 1, \ldots, n$. By Lemma 4(2), this means that A and B have the same j-th column for each $j = 1, \ldots, n$, which means $A = B$. □

Theorem 2.9. *Let $A \in M_{m\times n}(\mathbb{F})$. Then the function $L_A : \mathbb{F}^n \to \mathbb{F}^m$ is a linear transformation.*

Proof. By Proposition 2, it is enough to prove $L_A(c\mathbf{x} + \mathbf{y}) = cL_A(\mathbf{x}) + L_A(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ and $c \in \mathbb{F}$. Write $\mathbf{x} = (x_1, \ldots, x_n)^T$ and $\mathbf{y} = (y_1, \ldots, y_n)^T$ and also write $A = [a_1 \;\; a_2 \;\; \cdots \;\; a_n]$, meaning that $a_1, \ldots, a_n \in \mathbb{F}^m$ are the columns of A. Then $c\mathbf{x} + \mathbf{y} = (cx_1 + y_1, \ldots, cx_n + y_n)^T$ and

$$\begin{aligned}
L_A(c\mathbf{x} + \mathbf{y}) &= A(c\mathbf{x} + \mathbf{y}) \\
&= (cx_1 + y_1)a_1 + (cx_2 + y_2)a_2 + \cdots + (cx_n + y_n)a_n \qquad \text{(by Lemma 4(1))} \\
&= c(x_1a_1 + \cdots + x_na_n) + (y_1a_1 + \cdots + y_na_n) \\
&= c(A\mathbf{x}) + A\mathbf{y} \qquad \text{(by Lemma 4(1) again)} \\
&= cL_A(\mathbf{x}) + L_A(\mathbf{y}).
\end{aligned}$$

□

We end this section with a "meta" result. Fix a field $\mathbb{F}$ and positive integers $m, n \geq 1$. We have seen in the previous theorem that each $A \in M_{m\times n}(\mathbb{F})$ gives us a linear transformation $L_A : \mathbb{F}^n \to \mathbb{F}^m$, which is therefore an *element* of $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$. Thus we get a function from $M_{m\times n}(\mathbb{F})$ to $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$, namely, the function which sends each matrix A to its corresponding linear transformation L_A. Let's denote this function by L. That is, $\mathsf{L} : M_{m\times n}(\mathbb{F}) \to \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$ is given by $\mathsf{L}(A) = L_A$.

Note that both the domain and codomain of L are vector spaces over $\mathbb{F}$. Are you wondering whether L is linear? It is:

Proposition 4. *In the above situation, $\mathsf{L} : M_{m\times n}(\mathbb{F}) \to \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$ is a one-to-one linear transformation.*

Proof. We first show that L is linear. By Proposition 2, it suffices to show $\mathsf{L}(cA + B) = c\mathsf{L}(A) + \mathsf{L}(B)$ for any matrices $A, B \in M_{m\times n}(\mathbb{F})$ and scalar $c \in \mathbb{F}$. In other words, we must show $L_{cA+B} = cL_A + L_B$. Since both L_{cA+B} and $cL_A + L_B$ are functions, to show they are equal we must show that they have

the same value at any $\mathbf{x}$ in their common domain (which is $\mathbb{F}^n$). So let $\mathbf{x} \in \mathbb{F}^n$. We must show $L_{cA+B}(\mathbf{x}) = (cL_A + L_B)(\mathbf{x})$. Well, write A and B in terms of their columns, so $A = [a_1 \;\; a_2 \;\; \cdots \;\; a_n]$ and $B = [b_1 \;\; b_2 \;\; \cdots \;\; b_n]$. Then $cA = [ca_1 \;\; ca_2 \;\; \cdots \;\; ca_n]$ and so $cA + B = [ca_1 + b_1 \;\; ca_2 + b_2 \;\; \cdots \;\; ca_n + b_n]$. So

$$\begin{aligned} L_{cA+B}(\mathbf{x}) \;=\; (cA+B)\mathbf{x} &= x_1(ca_1+b_1) + x_2(ca_2+b_2) + \cdots + x_n(ca_n+b_n) \qquad \text{(Lemma 4(1))} \\ &= c(x_1a_1 + \cdots + x_na_n) + (x_1b_1 + \cdots + x_nb_n) \\ &= c(A\mathbf{x}) + B\mathbf{x} \;=\; cL_A(\mathbf{x}) + L_B(\mathbf{x}) \;=\; (cL_A + L_B)(\mathbf{x}). \end{aligned}$$

Since $\mathbf{x}$ was arbitrary, this proves $L_{cA+B} = cL_A + L_B$ as required.

Next we show that L is one-to-one. Rather than using Lemma 3, we will show directly that if $A, B \in M_{m\times n}(\mathbb{F})$ and $L_A = L_B$, then $A = B$. So assume $L_A = L_B$. That means $L_A(\mathbf{x}) = L_B(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}^n$, which means $A\mathbf{x} = B\mathbf{x}$ for all $\mathbf{x} \in \mathbb{F}^n$. Hence $A = B$ by the Matrix Equality Theorem (Corollary 2.8.1). □

Remark. We'll see later that L is actually an isomorphism from $M_{m\times n}(\mathbb{F})$ to $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$.

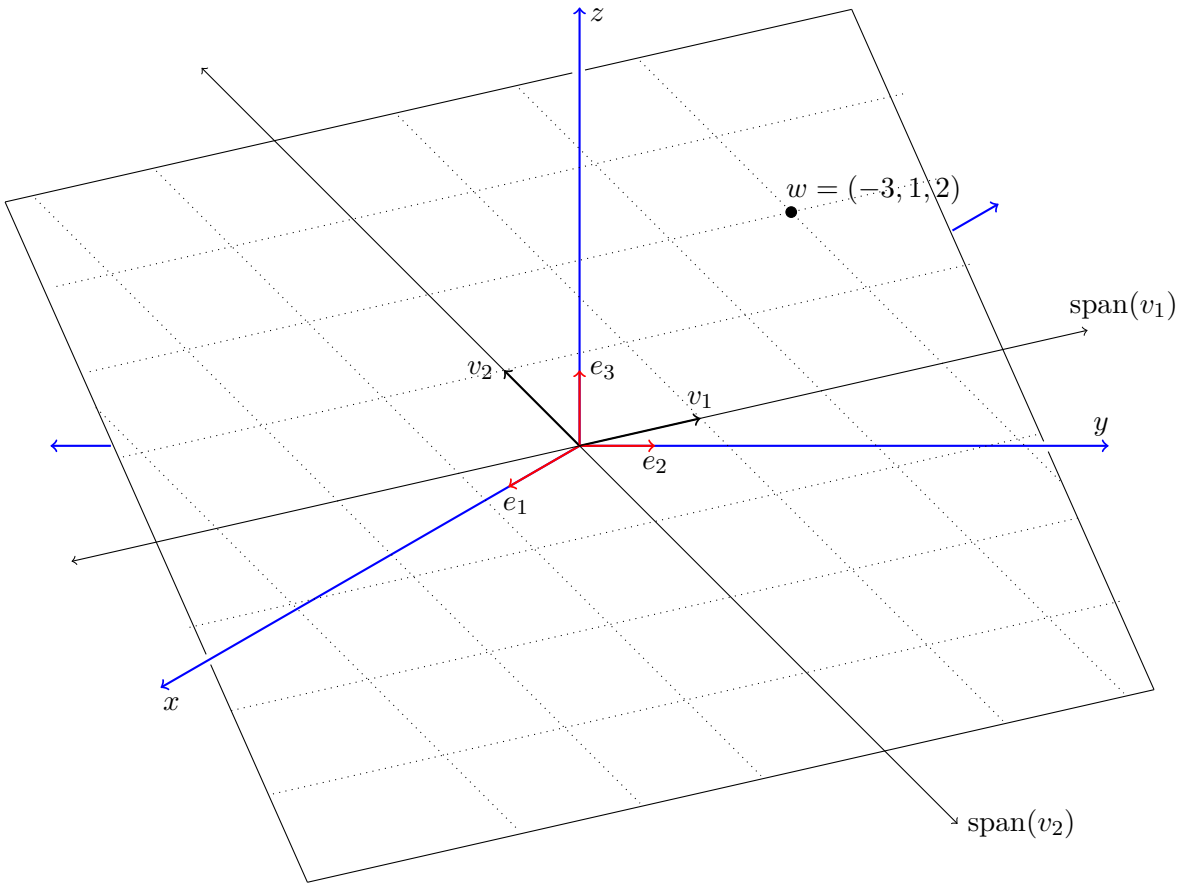
2.2 Coordinates

One way that bases for a vector space are useful is that they allow us to define the dimension of the vector space. A second way that bases are useful is that they give us a way to express vectors in the space in terms of *coordinates*. Here is an example of what we mean.

Example 29. Let W be the subset of $\mathbb{R}^3$ defined by the equation $x + y + z = 0$. That is,

$$W = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}.$$

We know that W is a plane in $\mathbb{R}^3$ through the origin, so W is a subspace of $\mathbb{R}^3$. Therefore W is a vector space in its own right. We also know by intuitive reasoning that $\dim(W) = 2$. It is not hard to find a basis for W. I will use the vectors $v_1 = (-1, 1, 0)$ and $v_2 = (0, -1, 1)$. Clearly v_1 and v_2 are both nonzero, and neither is a scalar multiple of the other. Therefore the set $\{v_1, v_2\}$ is linearly independent by Theorem 1.5. It's also easy to check that v_1 and v_2 both are in W, so $\{v_1, v_2\}$ is a linearly independent set *in* W. Since the number of vectors in this set equals the dimension of W, it follows by Corollary 1.9.2(2) that $\{v_1, v_2\}$ is a basis for W. Here is a picture depicting W in $\mathbb{R}^3$ with v_1 and v_2 shown.



In this picture, span(v_1) and span(v_2) are the lines through the origin containing v_1 and v_2 respectively. Note that the picture also contains a dotted line parallel to span(v_1) and passing through the vector v_2; this dotted line is simply the coset $v_2 + \text{span}(v_1)$. The picture also shows other cosets of the form $kv_2 + \text{span}(v_1)$ with $k \in \mathbb{Z}$.

Similarly, the dotted line parallel to span(v_2) and passing through v_1 is the coset $v_1 + \text{span}(v_2)$. The picture shows this coset as well as other cosets of the form $\ell v_1 + \text{span}(v_2)$ with $\ell \in \mathbb{Z}$.

Now these dotted lines should give the idea of a *grid structure* imposed on W. The two families of dotted lines making this grid are not at right angles to each other, but that is unimportant. Also, the distance separating the lines parallel to span(v_2) is not the same as the distance separating the lines parallel to span(v_1); this is also not important. The important thing is that the two families of parallel dotted lines give a way to assign *addresses* to each vector in W.

For example, consider the vector $w = (-3, 1, 2)$. It is easy to check that w is in W (since its entries sum to 0). Since $\{v_1, v_2\}$ is a basis for W, it follows by applying Theorem 1.6 that w can be *uniquely* written in the form $w = a_1v_1 + a_2v_2$, i.e., the scalars (real numbers) a_1, a_2 making this equation true are uniquely determined by w. By writing out the equation $w = a_1v_1 + a_2v_2$, we can solve for a_1 and a_2; doing that gives $a_1 = 3$ and $a_2 = 2$, and we can check this by calculating

$$3v_1 + 2v_2 \;=\; 3(-1, 1, 0) + 2(0, -1, 1) \;=\; (-3, 3 - 2, 2) \;=\; (-3, 1, 2) \;=\; w \quad \checkmark$$

But what is the *significance* of these numbers $a_1 = 3$ and $a_2 = 2$? This is where the grid comes in. These numbers tell us where "in the grid" the vector w lies: 3 "units" in the direction of v_1, and 2

"units" in the direction of v_2. We can think of the pair $(3,2)$ as being the "address" of w (with respect to the grid system defined by v_1 and v_2). We call the pair $(3,2)$, or the column vector $(3,2)^T = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$, the *coordinates* of w *with respect to* the basis $\{v_1, v_2\}$.

Now here are the formal definitions.

Definition 24. *Let V be a finite dimensional vector space. An ordered basis for V is a basis $\{v_1, \ldots, v_n\}$ endowed with a specific order.*

Example 30.

1. In $\mathbb{F}^3$, the set $\alpha = \{e_1, e_2, e_3\}$ is an ordered basis, $\beta = \{e_2, e_3, e_1\}$ is another ordered basis, and $\alpha \neq \beta$. Here $e_1 = (1,0,0)^T, e_2 = (0,1,0)^T, e_3 = (0,0,1)^T$.
2. The set $\{e_1, \ldots, e_n\}$ is called the standard ordered basis for $\mathbb{F}^n$, where $e_k = (0, \ldots, 0, 1, 0, \ldots, 0)^T$ and the k-th index of e_k is 1.
3. The set $\{1, x, \ldots, x^n\}$ is the standard ordered basis for $P_n(\mathbb{F})$.

Definition 25. *Let $\beta = \{u_1, \ldots, u_n\}$ be an ordered basis for a finite dimensional vector space V. For $x \in V$, let $a_1, \ldots, a_n$ be the unique scalars such that $x = \sum_{k=1}^{n} a_k u_k$. We define the coordinate vector of x relative to β to be*

$$[x]_\beta := \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{F}^n.$$

Example 31.

1. Let $V = P_2(\mathbb{R})$, $\beta = \{1, x, x^2\}$, and $p(x) = 2 - 3x + 4x^2 \in V$. Then $[p(x)]_\beta = \begin{bmatrix} 2 \\ -3 \\ 4 \end{bmatrix}$.
2. Let $V = M_{2\times 2}(\mathbb{R})$, $\beta = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$. Then $\begin{bmatrix} a & b \\ c & d \end{bmatrix}_\beta = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$.
3. Let $V = \mathbb{F}^n$ and let $\beta = \{e_1, \ldots, e_n\}$ be the standard ordered basis. Then for any $\mathbf{x} \in \mathbb{F}^n$, $[\mathbf{x}]_\beta = \mathbf{x}$. (Try it!)
4. Let $V = \mathbb{R}^2$, $\beta = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ -1 \end{bmatrix} \right\}$. Find $\begin{bmatrix} 8 \\ -1 \end{bmatrix}_\beta$. (Answered in the video modules).

The next result is perhaps not surprising, but will be very useful in the next section.

Theorem 2.10. *Let V be an n-dimensional vector space over $\mathbb{F}$ and let β be an ordered basis for V. The map $[\ ]_\beta : V \to \mathbb{F}^n$ is an isomorphism.*

Proof. Shown in the video modules. □

2.3 Matrix Representation of a Linear Transformation

Let V and W be vector spaces where $\dim V = n$. Let $\{v_1, \ldots, v_n\}$ be a basis for V, let $T : V \to W$ be a linear transformation, and define $w_1, \ldots, w_m \in W$ by $w_i = T(v_i)$. Recall that Theorem 2.1 says in this situation that T is the *unique* linear transformation from V to W sending $v_i \mapsto w_i$ for all $i = 1, \ldots, n$. In other words, T is completely determined by its values $T(v_1), T(v_2), \ldots, T(v_n)$ at the basis elements. Next, we will define a matrix representation of T using coordinate vectors of $T(v_1), T(v_2), \ldots, T(v_n)$ relative to an ordered basis for W.

Definition 26. *Let V and W be finite dimensional vector spaces over $\mathbb{F}$ and let $T : V \to W$ be a linear transformation. Let $\beta = \{v_1, \ldots, v_n\}$ and $\gamma = \{w_1, \ldots, w_m\}$ be ordered bases for V and W, respectively. The matrix representation of T in the ordered bases β and γ is the matrix $[T]_\beta^\gamma$ with entries from $\mathbb{F}$ defined as follows:*

$$[T]_\beta^\gamma = \begin{bmatrix} [T(v_1)]_\gamma & [T(v_2)]_\gamma & \cdots & [T(v_n)]_\gamma \end{bmatrix}.$$

When $T : V \to V$ is linear and β is an ordered basis of the finite-dimensional vector space V, denote $[T]_\beta = [T]_\beta^\beta$.

Remark 12. Under the same assumption as Definition 26 for $T : V \to W$, if we denote $A = [T]_\beta^\gamma$, then

1. $A \in M_{m\times n}(\mathbb{F})$, where (# rows of A) $= m = \dim W$ and (# columns of A) $= n = \dim V$.
2. For all $1 \le j \le n$, the j-th column of A is $[T(v_j)]_\gamma$. If we write $A = (a_{ij})$ as usual, then the j-th column of A is $(a_{1j}, a_{2j}, \ldots, a_{mj})^T$, so by the definition of $[T(v_j)]_\gamma$ we have

$$T(v_j) = \sum_{k=1}^{m} a_{kj} w_k.$$

Example 32. Consider $T : P_2(\mathbb{R}) \to \mathbb{R}^2$, $T(a + bx + cx^2) = \begin{bmatrix} a \\ b + 4c \end{bmatrix}$. We can verify that T is linear. Let $\beta = \{1, x + 1, (x + 1)^2\}$ and $\gamma = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$. Find $[T]_\beta^\gamma$. (Answered in video modules).

Example 33. Let $A \in M_{m\times n}(\mathbb{F})$ and consider $L_A : \mathbb{F}^n \to \mathbb{F}^m$. Let β be the standard ordered basis for $\mathbb{F}^n$ and let γ be the standard ordered basis for $\mathbb{F}^m$. Then $[L_A]_\beta^\gamma = A$. (This will be explained in the videos.)

One of the ways that matrix representations of a linear transformation are useful is that they enable a description of the action of the transformation using the language of matrix-vector multiplication. More precisely, suppose V and W are finite-dimensional vector spaces over $\mathbb{F}$, β and γ are ordered bases for V and W respectively, and $T : V \to W$ is linear. Now let $x \in V$ be given, and suppose that we want to know what is $T(x)$. In principle, it will be enough to know the coordinates of $T(x)$ relative to γ (note that $T(x)$ is a vector in W). The next theorem says that you can find the coordinates of $T(x)$ (relative to γ) by multiplying the coordinate vector of x (relative to β) by the matrix representing T (for β and γ).

Theorem 2.11. *Let $T : V \to W$ be linear and $\beta = \{v_1, \ldots, v_n\}$ and $\gamma = \{w_1, \ldots, w_m\}$ be ordered bases of V and W, respectively. Then*

$$[T(x)]_\gamma = [T]^\gamma_\beta \cdot [x]_\beta, \quad \forall x \in V.$$

Proof. Take $x \in V$. Then $x = \sum_{k=1}^{n} a_k v_k$, where $[x]_\beta = (a_1, \ldots, a_n)^T$. Since T is linear,

$$T(x) = T\left(\sum_{k=1}^{n} a_k v_k\right) = \sum_{k=1}^{n} a_k T(v_k).$$

Therefore,

$$[T(x)]_\gamma = \left[\sum_{k=1}^{n} a_k T(v_k)\right]_\gamma = \sum_{k=1}^{n} a_k [T(v_k)]_\gamma \qquad \text{by linearity of } [\ ]_\gamma, \text{ see Theorem 2.10}$$

Note that the last sum in the above equation is a linear combination of the columns of $[T]^\gamma_\beta$, using the entries of $[x]_\beta$ as coefficients. Thus by Lemma 4(1), this sum is equal to the matrix-vector product $[T]^\gamma_\beta \cdot [x]_\beta$. □

We end this section with a "meta" result for matrix representations. Note the similarities and differences with Proposition 4.

Proposition 5. *Let V and W be finite dimensional vector spaces over $\mathbb{F}$ and let β and γ be ordered bases of V and W, respectively.*

1. *For $T, U \in \mathcal{L}(V, W)$ and $c \in \mathbb{F}$, we have*

$$[T + U]^\gamma_\beta = [T]^\gamma_\beta + [U]^\gamma_\beta, \quad [cT]^\gamma_\beta = c[T]^\gamma_\beta.$$

2. *For every $C \in M_{m\times n}$ there exists a unique $T \in \mathcal{L}(V, W)$ such that $[T]^\gamma_\beta = C$.*

In other words, the map $[\ ]^\gamma_\beta : \mathcal{L}(V, W) \to M_{m\times n}(\mathbb{F})$ is an isomorphism of vector spaces, where $m = \dim(W)$ and $n = \dim(V)$.

Proof Sketch. (1) Suppose $\beta = \{v_1, \ldots, v_n\}$.

$$\begin{aligned}
[T + U]^\gamma_\beta &= \Big[[(T + U)(v_1)]_\gamma \quad [(T + U)(v_2)]_\gamma \quad \cdots \quad [(T + U)(v_n)]_\gamma\Big] \\
&= \Big[[T(v_1) + U(v_1)]_\gamma \quad [T(v_2) + U(v_2)]_\gamma \quad \cdots \quad [T(v_n) + U(v_n)]_\gamma\Big] \quad \text{(by definition of } T + U) \\
&= \Big[\Big([T(v_1)]_\gamma + [U(v_1)]_\gamma\Big) \quad \Big([T(v_2)]_\gamma + [U(v_2)]_\gamma\Big) \quad \cdots \quad \Big([T(v_n)]_\gamma + [U(v_n)]_\gamma\Big)\Big] \quad \text{(by linearity of } [\ ]_\gamma) \\
&= \Big[[T(v_1)]_\gamma \quad [T(v_2)]_\gamma \quad \cdots \quad [T(v_n)]_\gamma\Big] + \Big[[U(v_1)]_\gamma \quad [U(v_2)]_\gamma \quad \cdots \quad [U(v_n)]_\gamma\Big] \\
&= [T]^\gamma_\beta + [U]^\gamma_\beta.
\end{aligned}$$

(2) If $[T]^\gamma_\beta = [U]^\gamma_\beta$, then for every $j = 1, \ldots, n$, $[T]^\gamma_\beta$ and $[U]^\gamma_\beta$ have the same j-th column. This means $[T(v_j)]_\gamma = [U(v_j)]_\gamma$, and since the function $[\ ]_\gamma : W \to \mathbb{F}^m$ is a bijection (Theorem 2.10) we get $T(v_j) = U(v_j)$. Thus T and U agree on the vectors in the basis β. By Theorem 2.1, $T = U$. This proves $[\ ]^\gamma_\beta$ is one-to-one. To prove it is onto, let $C = [c_1 \ \ c_2 \ \cdots \ c_n] \in M_{m\times n}(\mathbb{F})$ be given. For each $j = 1, \ldots, n$ let $w_j \in W$ be (unique) the vector satisfying $[w_j]_\gamma = c_j$. By Theorem 2.10, there exists a (unique) linear transformation $T : V \to W$ satisfying $T(v_j) = w_j$ for $j = 1, \ldots, n$. This T satisfies $[T]^\gamma_\beta = C$. □

Corollary 2.11.1. The map $\mathsf{L} : M_{m\times n}(\mathbb{F}) \to \mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)$ is an isomorphism.

Proof sketch. We already know from Proposition 4 that L is a one-to-one linear transformation, so it just remains to prove that it is onto. Applying Proposition 5 to $V = \mathbb{F}^n$, $W = \mathbb{F}^m$ tells us that $\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m) \cong M_{m\times n}(\mathbb{F})$; hence $\dim(\mathcal{L}(\mathbb{F}^n, \mathbb{F}^m)) = \dim(M_{m\times n}(\mathbb{F})) = mn$ by Theorem 2.6. So L is a one-to-one linear transformation between vector spaces of the same finite dimension. It follows by Theorem 2.7 that L is onto. □

2.4 Matrix Multiplication and Composition of Linear Transformations

In this section, we will define matrix multiplication and explain how it is connected to the composition of linear transformations.

Definition 27. *Let $\mathbb{F}$ be a field. Suppose $A \in M_{m\times n}(\mathbb{F})$ and $B \in M_{n\times p}(\mathbb{F})$. (Note that the number of columns in A equals the number of rows in B; this is required.) The **matrix product** AB is the $m \times p$ matrix $C \in M_{m\times p}(\mathbb{F})$ whose row-i, column-j entry is the sum of products formed multiplying the entries in the i-th row of A with the entries in the j-th column of B. That is,*

$$\begin{pmatrix} a_{11} & \cdots & a_{1t} & \cdots & a_{1n} \\ & & \vdots & & \\ \boxed{a_{i1} & \cdots & a_{it} & \cdots & a_{in}} \\ & & \vdots & & \\ a_{m1} & \cdots & a_{mt} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & & \boxed{b_{1j}} & & b_{1p} \\ \vdots & & \vdots & & \vdots \\ b_{t1} & \cdots & b_{tj} & \cdots & b_{tp} \\ \vdots & & \vdots & & \vdots \\ b_{n1} & & b_{nj} & & b_{np} \end{pmatrix} = \begin{pmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1p} \\ \vdots & & \vdots & & \vdots \\ c_{i1} & \cdots & \boxed{c_{ij}} & \cdots & c_{ip} \\ \vdots & & \vdots & & \vdots \\ c_{m1} & \cdots & c_{mj} & \cdots & c_{mp} \end{pmatrix}$$

where each entry c_{ij} of the product is given by $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$, or in summation notation,

$$c_{ij} = \sum_{t=1}^{n} a_{it}b_{tj}.$$

If A and B are matrices and the number of columns of A does not *equal the number of rows of B, then AB is not defined.*

Remark 13.

1. If $p = 1$, so B and AB are column vectors, then the definition above is the matrix-vector product defined earlier.

2. In general (i.e., when B has several columns), B and AB have the same number of columns, and the j-th column of AB is obtained by multiplying A by the j-th column of B. That is, if $B = [b_1 \;\; b_2 \;\; \cdots \;\; b_p]$ and $AB = C = [c_1 \;\; c_2 \;\; \cdots \;\; c_p]$, then $c_j = Ab_j$ for $j = 1, \ldots, p$.

3. Combining the previous item with Lemma 4(1), we see that the j-th column of AB is the linear combination of the columns of A formed using the entries in the j-th column of B as coefficients.

Example 34. 1. Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \in M_{2\times 3}(\mathbb{Q})$ and $B = \begin{bmatrix} 2 & 1 & 0 & -1 \\ 3 & 6 & 5 & 4 \\ -2 & 0 & 1 & 2 \end{bmatrix} \in M_{3\times 4}(\mathbb{Q})$. Then

$$AB = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} 2 & 1 & 0 & -1 \\ 3 & 6 & 5 & 4 \\ -2 & 0 & 1 & 2 \end{bmatrix} = C = [c_1 \;\; c_2 \;\; c_3 \;\; c_4] \qquad \text{where}$$

$$c_1 = 2\begin{bmatrix} 1 \\ 4 \end{bmatrix} + 3\begin{bmatrix} 2 \\ 5 \end{bmatrix} + (-2)\begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 2 \\ 11 \end{bmatrix} \qquad c_2 = 1\begin{bmatrix} 1 \\ 4 \end{bmatrix} + 6\begin{bmatrix} 2 \\ 5 \end{bmatrix} + 0\begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 13 \\ 34 \end{bmatrix}$$

$$c_3 = 0\begin{bmatrix} 1 \\ 4 \end{bmatrix} + 5\begin{bmatrix} 2 \\ 5 \end{bmatrix} + 1\begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 13 \\ 31 \end{bmatrix} \qquad c_4 = (-1)\begin{bmatrix} 1 \\ 4 \end{bmatrix} + 4\begin{bmatrix} 2 \\ 5 \end{bmatrix} + 2\begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 13 \\ 28 \end{bmatrix}.$$

Hence $AB = \begin{bmatrix} 2 & 13 & 13 & 13 \\ 11 & 34 & 31 & 28 \end{bmatrix}$. Note that AB has the same number of rows as A, and the same number of columns as B. Also note that every column of AB is a linear combination of the columns of A.

2. Let $A \in M_{3\times 2}(\mathbb{R})$ and $B \in M_{2\times 4}(\mathbb{R})$. Then AB is defined (it is a 3×4 matrix) but BA is not defined.

3. Let $A \in M_{2\times 3}(\mathbb{F})$ and $B \in M_{3\times 2}(\mathbb{F})$. Both AB and BA are defined, but they cannot be equal since AB is a 2×2 matrix while BA is a 3×3 matrix.

4. Let $A = \begin{bmatrix} 1 & 2 \\ 1 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$. Both AB and BA are defined and are 2×2 matrices. That does not imply, however, that they are equal to each other. And if we calculate, we find that $AB = \begin{bmatrix} 4 & 2 \\ 1 & -1 \end{bmatrix}$ while $BA = \begin{bmatrix} 2 & 4 \\ 2 & 1 \end{bmatrix}$, so $AB \neq BA$ in this example.

Except for the facts that matrix products are not always defined, and that $AB = BA$ may fail, matrix products satisfy many of the other "usual" laws of arithmetic. We will first give some notation and then give a Lemma stating these laws.

Some matrix notations:

- We usually use O to denote a zero matrix, i.e., a matrix in which every entry is 0. If we need to specify its number of rows and columns, then we may write $O_{m\times n}$.
- For each $n \geq 1$ we let I_n denote the $n \times n$ identity matrix. This is the matrix whose (i, j)-entry is given by the Kronecker delta $\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$. For example, $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Lemma 5. *1. $A(B + C) = AB + AC$, where $A \in M_{m\times n}(\mathbb{F})$ and $B, C \in M_{n\times p}(\mathbb{F})$.*

2. $(D+E)A = DA + EA$, *where* $A \in M_{m\times n}(\mathbb{F})$ *and* $D, E \in M_{q\times m}(\mathbb{F})$.

3. $\alpha(AB) = (\alpha A)B = A(\alpha B) \quad \forall \alpha \in \mathbb{F}$, *where* $A \in M_{m\times n}(\mathbb{F})$ *and* $B \in M_{n\times p}(\mathbb{F})$.

4. $(AB)^t = B^t A^t$, *where* $A \in M_{m\times n}(\mathbb{F})$ *and* $B \in M_{n\times p}(\mathbb{F})$.

5. $I_m A = AI_n = A$, *where* $A \in M_{m\times n}(\mathbb{F})$.

6. $AO_{n\times p} = O_{m\times p}$ *and* $O_{q\times m}A = O_{q\times n}$, *where* $A \in M_{m\times n}(\mathbb{F})$.

Proof. Some of (1)–(4) will proved in the videos; other parts are left as an exercise.
(5). Note that the columns of I_n are exactly the standard basis vectors $e_1, e_2, \ldots, e_n$ for $\mathbb{F}^n$. Thus $AI_n = A[e_1 \;\; e_2 \;\; \cdots \;\; e_n] = [Ae_1 \;\; Ae_2 \;\; \cdots \;\; Ae_n]$ by Remark 13(2). Write $A = [a_1 \;\; a_2 \;\; \cdots \;\; a_n]$. We know from Lemma 4(2) that Ae_j equals the j-th column of A, so $[Ae_1 \;\; Ae_2 \;\; \cdots \;\; Ae_n] = [a_1 \;\; a_2 \;\; \cdots \;\; a_n] = A$. This proves $AI_n = A$. Now we can use item (4) and the fact that $I_m^t = I_m$ to deduce $I_m A = A$:

$$(I_m A)^t = A^t I_m^t = A^t I_m = A^t \;\Rightarrow\; I_m A = ((I_m A)^t)^t = (A^t)^t = A. \qquad \square$$

Remark. The previous Lemma gives most of the important algebraic laws about matrix addition and multiplication, but it doesn't mention what is perhaps the most important law: the *associative law* $A(BC) = (AB)C$ for multiplication (when all the products are defined). The story around this law is actually quite interesting and is connected to composition of linear transformations and matrix representations of linear transformations, so we turn now to those topics.

Theorem 2.12. *Let* $T : V \to W$ *and* $U : W \to Z$ *be linear transformations between vector spaces. Then the composition function* $U \circ T : V \to Z$, *given by* $(U \circ T)(x) = U(T(x))$ *for* $x \in V$, *is also linear.*

Proof. Exercise. $\square$

Remark: We will usually denote $U \circ T$ by UT.

Suppose again that $T : V \to W$ and $U : W \to Z$ are linear transformations, but this time also suppose that V, W, Z are finite-dimensional, say $\dim(V) = p$, $\dim(W) = n$, and $\dim(Z) = m$. Also assume that

$$\begin{aligned} \alpha = \{v_1, \ldots, v_p\} &\qquad \text{is an ordered basis for } V \\ \beta = \{w_1, \ldots, w_n\} &\qquad \text{is an ordered basis for } W \\ \gamma = \{z_1, \ldots, z_m\} &\qquad \text{is an ordered basis for } Z \end{aligned}$$

Let $\mathbb{F}$ be the field over which V, W, Z are vector spaces. Using α, β, γ we get matrix representations for T, U and UT, namely,

$$\begin{aligned} [T]_\alpha^\beta &\in M_{n\times p}(\mathbb{F}) \\ [U]_\beta^\gamma &\in M_{m\times n}(\mathbb{F}) \\ [UT]_\alpha^\gamma &\in M_{m\times p}(\mathbb{F}). \end{aligned}$$

Note also that the sizes of $[U]_\beta^\gamma$ and $[T]_\alpha^\beta$ are compatible so their matrix product $[U]_\beta^\gamma \cdot [T]_\alpha^\beta$ is defined. Also note that the product of these two matrices will be an $m \times p$ matrix, same as $[UT]_\alpha^\gamma$. Coincidence?

Theorem 2.13 (Matrix of Composition of Linear Transformations)**.** *Let V, W, and Z be finite dimensional vector spaces having ordered bases $\alpha = \{v_1, \ldots, v_p\}$, $\beta = \{w_1, \ldots, w_n\}$, and $\gamma = \{z_1, \ldots, z_m\}$, respectively. Let $T : V \to W$ and $U : W \to Z$ be linear transformations. Denote $A = [U]_\beta^\gamma \in M_{m\times n}(\mathbb{F})$, $B = [T]_\alpha^\beta \in M_{n\times p}(\mathbb{F})$, and $C = [UT]_\alpha^\gamma \in M_{m\times p}(\mathbb{F})$. Then $C = AB$. That is, $[UT]_\alpha^\gamma = [U]_\beta^\gamma \cdot [T]_\alpha^\beta$.*

Proof. Both sides are $m \times p$ matrices. We will show that, for each $j = 1, \ldots, p$, the j-th columns of the left-hand-side and right-hand-side matrices are equal. On the one hand, the j-th column of $[UT]_\alpha^\gamma$ is the coordinate vector $[UT(v_j)]_\gamma$ by definition of the matrix representation $[UT]_\alpha^\gamma$. On the other hand, write $[T]_\alpha^\beta = B = [b_1 \;\; b_2 \;\; \cdots \;\; b_p]$. By Remark 13(2), the j-th column of $[U]_\beta^\gamma \cdot [T]_\alpha^\beta$ is $[U]_\beta^\gamma \cdot b_j$, which equals

$$\begin{aligned}
[U]_\beta^\gamma \cdot b_j &= [U]_\beta^\gamma \cdot [T(v_j)]_\beta && \text{by definition of } [T]_\alpha^\beta \\
&= [U]_\beta^\gamma \cdot [x]_\beta && \text{let } x := T(v_j) \text{ to simplify notation} \\
&= [U(x)]_\gamma && \text{by Theorem 2.11} \\
&= [U(T(v_j))]_\gamma && \text{recalling what } x \text{ is} \\
&= [UT(v_j)]_\gamma && \text{definition of } UT.
\end{aligned}$$

Thus $[UT]_\alpha^\gamma$ and $[U]_\beta^\gamma \cdot [T]_\alpha^\beta$ have the same j-th columns. Since j was arbitrary, $[UT]_\alpha^\gamma$ and $[U]_\beta^\gamma \cdot [T]_\alpha^\beta$ are the same matrix. □

The previous theorem shows that matrix multiplication encodes the composition of linear transformations. In our last result of this section, we will exploit this fact to prove that matrix multiplication is associative.

Corollary 2.13.1.

1. $L_{AB} = L_A L_B$, whenever $A \in M_{m\times n}(\mathbb{F})$ and $B \in M_{n\times p}(\mathbb{F})$.
2. $A(BC) = (AB)C$, whenever the sizes of A, B, C make all the matrix products defined.

Proof Sketch. 1. Let α be the *standard* ordered basis for $\mathbb{F}^p$, let β be the *standard* ordered basis for $\mathbb{F}^n$, and let γ be the *standard* ordered basis for $\mathbb{F}^m$. Then $[L_A]_\beta^\gamma = A$, $[L_B]_\alpha^\beta = B$, and $[L_{AB}]_\alpha^\gamma = AB$ by Example 33. On the other hand,

$$\begin{aligned}
[L_A L_B]_\alpha^\gamma &= [L_A]_\beta^\gamma \cdot [L_B]_\alpha^\beta \qquad \text{(Theorem 2.13)} \\
&= AB = [L_{AB}]_\alpha^\gamma.
\end{aligned}$$

Since the map $[\;\;]_\alpha^\gamma$ is one-to-one (Corollary 2.11.1), we get $L_A L_B = L_{AB}$.

2. In order to prove $A(BC) = (AB)C$, we will first prove $L_{A(BC)} = L_{(AB)C}$. Using (1), we get that

$$L_{A(BC)} = L_A L_{BC} = L_A(L_B L_C) \qquad \text{while} \qquad L_{(AB)C} = L_{AB} L_C = (L_A L_B) L_C.$$

But $L_A(L_B L_C) = (L_A L_B) L_C$ since composition of functions is associative (this is the point!). This proves $L_{A(BC)} = L_{(AB)C}$. Since L is one-to-one (Proposition 4), it follows that $A(BC) = (AB)C$.

□

2.5 Invertibility and Isomorphisms

From Section 2.3, we know that every linear transformation can be represented by a matrix and the matrix depends on the choice of bases. We also studied one-to-one transformations, onto transformations, and isomorphisms. A natural question arises: What do the corresponding matrices look like? In this section, we will show the relation between isomorphisms and invertible matrices and study fundamental properties of the matrix inverse operator.

Definition 28. *A square matrix $A \in M_{n\times n}(\mathbb{F})$ is invertible if there exists a matrix $B \in M_{n\times n}(\mathbb{F})$ such that $AB = BA = I_n$.*

Note that if such B exists, then B is uniquely determined by A. That is, if there exist $B, C \in M_{n\times n}(\mathbb{F})$ such that $AB = BA = I_n$ and $AC = CA = I_n$, then $B = C$. Indeed, we have

$$B = BI_n = B(AC) = (BA)C = I_nC = C.$$

Notation. The matrix B is called the inverse of A, and is denoted by A^{-1}.

Example 35. The matrix $A = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix}$ is invertible and its inverse is $B = \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix}$ since

$$AB = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} = I_2,$$

$$BA = \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} = I_2.$$

Before studying the relation between invertible matrices and isomorphisms, we first see the connection between isomorphism and inverse functions.

Definition 29. *Let $T : V \to W$ be a linear mapping between vector spaces V and W. If there exists a function $U : W \to V$ such that $UT = I_V$ and $TU = I_W$, then T is said to be invertible and U is said to be an inverse of T.*

Note that if a linear mapping T is invertible, then the inverse of T is unique and is denoted by T^{-1}. In addition, we can prove that T^{-1} is also linear.

Lemma 6. *Suppose $T : V \to W$ is linear and invertible. Then the inverse of T is unique.*

Proof. Suppose there exist $U_1, U_2 : W \to V$ satisfying

$$U_1T = I_V, \quad TU_1 = I_W, \quad U_2T = I_V, \quad TU_2 = I_W.$$

Then

$$U_1 = U_1I_W = U_1(TU_2) = (U_1T)U_2 = I_VU_2 = U_2.$$

□

Theorem 2.14. *Let $T : V \to W$ be linear. Then T is invertible iff T is an isomorphism.*

Proof. ($\Rightarrow$) Suppose $x, y \in V$ such that $T(x) = T(y)$. Then

$$x = (T^{-1}T)(x) = T^{-1}(T(x)) = T^{-1}(T(y)) = (T^{-1}T)(y) = y.$$

Therefore, T is one-to-one.

On the other hand, let $z \in W$. From $TT^{-1} = I_W$, we have

$$z = I_W(z) = (TT^{-1})(z) = T(T^{-1}(z)).$$

Let $x = T^{-1}(z) \in V$. Then we have constructed $x \in V$ such that $T(x) = z$. Therefore, T is onto. Combining with the linearity of T, we conclude that T is an isomorphism.

($\Leftarrow$) Suppose T is an isomorphism. So T is one-to-one and onto. Then for every $z \in W$, there exists unique $x \in V$ such that $T(x) = z$. Define $U : W \to V, U(z) = x$. Then $UT = I_V$ and $TU = I_W$ (prove this!). Therefore, T is invertible. □

Lemma 7. *Suppose $T : V \to W$ is an isomorphism. Then T^{-1} is also linear.*

Proof. Take $y_1, y_2 \in W$ and $c \in \mathbb{F}$. Since T is one-to-one and onto, there exist unique $x_1, x_2 \in V$ such that $T(x_1) = y_1$ and $T(x_2) = y_2$. We have

$$\begin{aligned} T^{-1}(cy_1 + y_2) &= T^{-1}\left(cT(x_1) + T(x_2)\right) = T^{-1}(T(cx_1 + x_2)) = (T^{-1}T)(cx_1 + x_2) \\ &= cx_1 + x_2 = cT^{-1}(y_1) + T^{-1}(y_2). \end{aligned}$$

where the first equality is obtained by substituting $y_k = T(x_k)$, for $k = 1, 2$, the second equality is due to the linearity of T, the fourth equality holds because $T^{-1}T = I_V$, and the last equality is from $x_k = T^{-1}(y_k)$, for $k = 1, 2$. This completes the proof.

□

The following theorem indicates that we can associate each isomorphism with an invertible matrix.

Theorem 2.15. *Let V and W be finite dimensional vector spaces, and α and β be ordered bases of V and W, respectively. Let $T : V \to W$ be linear.*

1. *T is an isomorphism iff $[T]_\alpha^\beta$ is an invertible matrix.*
2. *In particular, if $A \in M_{n\times n}(\mathbb{F})$, then L_A is an isomorphism iff A is invertible.*

Proof. Let $A = [T]_\alpha^\beta$.

1. ($\Rightarrow$) Suppose T is an isomorphism. Then $V \cong W$. By Theorem 2.6, $\dim V = \dim W = n$. So A is a square matrix. By Theorem 2.14 and Lemma 7, $T^{-1} : W \to V$ is also linear. Let $B := [T^{-1}]_\beta^\alpha$, which is also an $n \times n$ matrix. Also,

$$AB = [T]_\alpha^\beta [T^{-1}]_\beta^\alpha \overset{Thm.\ 2.13}{=} [TT^{-1}]_\beta^\beta = [I_W]_\beta^\beta \overset{Exercise}{=} I_n.$$

   A similar proof shows $BA = [I_V]_\alpha^\alpha = I_n$. By Definition 28, A is an invertible matrix.

($\Leftarrow$) Suppose A is an invertible matrix with inverse A^{-1}. In particular, A must be square, say $n \times n$, so $\dim V = \dim W = n$. Let's first show that T is one-to-one. Let $x, y \in V$ such that $T(x) = T(y)$. By Theorem 2.11

$$A[x]_\alpha = [T]_\alpha^\beta [x]_\alpha = [T(x)]_\beta = [T(y)]_\beta = [T]_\alpha^\beta [y]_\alpha = A[y]_\alpha.$$

So $A[x]_\alpha = A[y]_\alpha$. Multiplying both sides by A^{-1} and using $A^{-1}A = I_n$, we have $[x]_\alpha = [y]_\alpha$. Hence $x = y$. Therefore, T is one-to-one. Since T is also linear and $\dim V = \dim W$, by Theorem 2.7, T is also onto, so is an isomorphism. This completes the proof.

2. Let $A \in M_{n\times n}(\mathbb{F})$. By part 1, L_A is an isomorphism iff $[L_A]_{\sigma_n}^{\sigma_n}$ is invertible where σ_n is the standard ordered basis for $\mathbb{F}^n$. By Example 33, $[L_A]_{\sigma_n}^{\sigma_n} = A$, which completes the proof.

□

From the proof of Theorem 2.15, we also see that if T is an isomorphism, $[T]_\alpha^\beta$ is an invertible matrix whose inverse is $[T^{-1}]_\beta^\alpha$. That is,

$$[T^{-1}]_\beta^\alpha = \left([T]_\alpha^\beta\right)^{-1}.$$

Next, we will study some properties of the matrix inverse operator.

Lemma 8. *1. If a matrix A is invertible, then A^{-1} is also invertible and $(A^{-1})^{-1} = A$.*

2. If A is invertible and $c \in \mathbb{F}$ with $c \neq 0$, then $(cA)^{-1} = \left(\frac{1}{c}\right) A^{-1}$.

3. If A is invertible, $(A^T)^{-1} = (A^{-1})^T$.

4. If $A, B \in M_{n\times n}(\mathbb{F})$ are invertible, then AB is also invertible and $(AB)^{-1} = B^{-1}A^{-1}$.

5. Conversely, if $A, B \in M_{n\times n}(\mathbb{F})$ and AB is invertible, then A and B are invertible matrices.

Proof. 1. Since A is invertible, A^{-1} exists. In particular, A^{-1} is a square matrix and $A^{-1}A = AA^{-1} = I_n$. Therefore, A is an inverse of A^{-1}. Hence, A^{-1} is also invertible. Due to the uniqueness of the matrix inverse, $A = (A^{-1})^{-1}$.

2. See the recorded module.

3. See the recorded module.

4. We have

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n,$$
$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n.$$

Therefore, $(AB)^{-1} = B^{-1}A^{-1}$.

5. Since AB is invertible, by Theorem 2.15, the mapping L_{AB} is invertible. By Theorem 2.14, $L_{AB} = L_A L_B$ is an isomorphism. Therefore, $L_A L_B$ is one-to-one and onto. Hence, L_A is surjective and L_B is injective (prove this!). Since L_A, L_B are both linear mappings from $\mathbb{F}^n$ to itself, by Theorem 2.7 L_A and L_B are isomorphisms. Therefore, A and B are invertible matrices.

□

Remark 14. Note that, we can find a pair of non-square matrices $A \in M_{m\times n}(\mathbb{R})$ and $B \in M_{n\times m}(\mathbb{R})$ with $m \neq n$ such that one of the products AB or BA is invertible. However, we can't find $A \in M_{m\times n}(\mathbb{R})$ and $B \in M_{n\times m}(\mathbb{R})$ with $m \neq n$ such that AB and BA are both invertible. For example, consider

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 5 & 7 \\ 2 & 3 \\ \pi & e \end{bmatrix}. \text{ Then } \quad BA = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \quad \text{is invertible.}$$

On the other hand, for any $A \in M_{3\times 2}(\mathbb{F})$ and $B \in M_{2\times 3}(\mathbb{F})$, the product AB will never be invertible. One way to prove this statement is by using the rank of a matrix, which we will study next week.

Next, we will study some useful criteria of invertible matrices.

Theorem 2.16 (Invertible Matrix Theorem, part 1)**.** *Let $A \in M_{n\times n}(\mathbb{F})$. The following statements are equivalent:*

1. *A is invertible.*
2. *There exists a matrix $C \in M_{n\times n}(\mathbb{F})$ such that $AC = I_n$.*
3. *There exists a matrix $B \in M_{n\times n}(\mathbb{F})$ such that $BA = I_n$.*

Proof. $(1 \Rightarrow 2)$ Suppose A is invertible. Then $C = A^{-1}$ satisfies the condition.

$(2 \Rightarrow 1)$. Since I_n is an invertible matrix and A and C are both square matrices, from Lemma 8 part 3, we conclude that A and C are invertible matrices. We have

$$A^{-1} = A^{-1}I_n = A^{-1}(AC) = (A^{-1}A)C = I_n C = C.$$

Similarly, we can prove $(1) \Leftrightarrow (3)$. □

We will add more statements to the Inverse Matrix Theorem througout the course.

2.6 The Change of Coordinate Matrix

Recall that every linear transformation is represented by a matrix. Furthermore, the matrix depends on the choice of basis. Therefore, if we change the basis, the matrix representation of the linear transformation is changed. On the other hand, one often uses a change of variables to simplify the appearance of an expression. In this section, we will study what the change of basis does to the matrix.

Theorem 2.17. *Let α and β be two ordered bases for a finite dimensional vector space V and let $Q = [I_V]_\alpha^\beta$. Then*

1. *Q is invertible, called the change of coordinate matrix from α to β.*

2. *For any $x \in V$, we have $[x]_\beta = Q[x]_\alpha$.*

Proof. 1. Since I_V is an isomorphism, by Theorem 2.15, Q is invertible.
2. By Theorem 2.11, we have:

$$[x]_\beta = [I_V(x)]_\beta = [I_V]_\alpha^\beta [x]_\alpha = Q[x]_\alpha.$$

□

Remark 15. Suppose V is a finite dimensional vector space over $\mathbb{F}$. Let $\alpha = \{v_1, \ldots, v_n\}$ and $\beta = \{w_1, \ldots, w_n\}$ be two ordered bases for V and $x \in V$. Then the change of coordinate matrix from α to β is

$$[I_V]_\alpha^\beta = \begin{bmatrix} [v_1]_\beta & \cdots & [v_n]_\beta \end{bmatrix}.$$

By comparing the j-th column on both sides (see also Remark 12), we have

$$v_j = \sum_{i=1}^{n} Q_{ij} w_i, \quad \forall 1 \leq j \leq n.$$

That is the column j-th of the change of coordinate matrix from $\alpha = \{v_1, \ldots, v_n\}$ to $\beta = \{w_1, \ldots, w_n\}$ is obtained by first writing v_j as a linear combination of vectors in β.

Example 36. Consider two ordered bases for $P_2(\mathbb{R})$, $\beta = \{1, x, x^2\}$ and $\alpha = \{x^2 + x + 4, 4x^2 - 3x + 2, 2x^2 + 3\}$. Find the change of coordinates matrix that changes α-coordinates into β-coordinates and find the change of coordinates matrix that change β-coordinates to α-coordinates.

Proof. See the recorded module. □

Theorem 2.18. *Let $T : V \to V$ be linear and V be a finite dimensional vector space. Let α and β be two ordered bases of V and Q be the change of coordinate matrix that changes α-coordinates into β-coordinates. Then*

$$[T]_\alpha = Q^{-1}[T]_\beta Q.$$

Proof. By Theorem 2.13, we have

$$Q[T]_\alpha = [I_V]_\alpha^\beta [T]_\alpha^\alpha = [I_V T]_\alpha^\beta = [T]_\alpha^\beta,$$

$$[T]_\beta Q = [T]_\beta^\beta [I_V]_\alpha^\beta = [T I_V]_\alpha^\beta = [T]_\alpha^\beta.$$

So $[T]_\beta Q = Q[T]_\alpha$. Since Q is invertible, Q^{-1} exits and

$$Q^{-1}[T]_\beta Q = Q^{-1}Q[T]_\alpha = I_n[T]_\alpha = [T]_\alpha.$$

□

Example 37. Let β be the standard ordered basis for $\mathbb{R}^2$ and let $\alpha = \left\{ \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$. Consider a linear mapping T on $\mathbb{R}^2$ defined by

$$T \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a + 2b \\ 2a + b \end{pmatrix}.$$

Given that $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$, find $[T]_\alpha$.

Proof. See the recorded module. □

Definition 30. *Let A and B be matrices in $M_{n\times n}(\mathbb{F})$. We say B is similar to A if there exists an invertible matrix Q such that $B = Q^{-1}AQ$.*

We will study the properties of similar matrices later in the course.

3 Elementary Matrix Operations and Systems of Linear Equations

In this chapter, we will investigate certain rank-preserving operations on matrices and analyze carefully how to solve systems of linear equations. We will also see other equivalent criteria for invertible matrices and study algorithms to find the inverse of a matrix (if exists).

3.1 Elementary Matrix Operations and Elementary Matrices

Definition 31. *Let A be an $m \times n$ matrix. The following operations of the rows (columns) of A are called an elementary row (column) operation:*

1. *Interchanging any two rows (columns) of A: $R_i \leftrightarrow R_j$*
2. *Multiplying any row (column) of A by a nonzero scalar: $R_i \leftarrow cR_i$*
3. *Adding any scalar multiple of a row (column) of A to another row (column): $R_i \leftarrow R_i + cR_j$.*

Example 38. Consider $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ -9 & -10 & -11 & -12 \end{bmatrix}$.

- Interchanging Row 1 and Row 3, we get

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ -9 & -10 & -11 & -12 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{bmatrix} -9 & -10 & -11 & -12 \\ 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 \end{bmatrix}.$$

- Multiplying Row 2 by 2, $R_2 \leftarrow 2 * R_2$, we get:

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ -9 & -10 & -11 & -12 \end{bmatrix} \xrightarrow{R_2 * 2} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 10 & 12 & 14 & 16 \\ -9 & -10 & -11 & -12 \end{bmatrix}.$$

- Adding 4*Row1 to Row 3, $R_3 \leftarrow R_3 + 4R_1$, we get:

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ -9 & -10 & -11 & -12 \end{bmatrix} \xrightarrow{R_3+4R_1} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ -5 & -2 & 1 & 4 \end{bmatrix}.$$

Definition 32. *An $n \times n$ elementary matrix is a matrix obtained by performing an elementary operation on I_n.*

Example 39. The 3×3 elementary matrix obtained by performing the elementary row operations in previous example (Example 25) on I_n are

$$I_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad I_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{bmatrix}.$$

Theorem 3.1. *Let $A \in M_{m\times n}(\mathbb{F})$ and suppose B is obtained from A by performing an elementary row operation. Then there exists an $m \times m$ elementary matrix E such that $B = EA$. In fact, E is obtained from I_m by performing the same elementary row operation as that which was performed on A to obtained B.*
Conversely, if E is an $m \times m$ elementary matrix, then EA is the matrix obtained from A by performing the same elementary row operation as that which produces E from I_m.

Note: we have a similar theorem for elementary column operations. In that case, E is an $n \times n$ matrix obtained from I_n by performing the elementary column operation and $B = AE$.

Theorem 3.2. *Let $A \in M_{m\times n}(\mathbb{F})$ and suppose B is obtained from A by performing an elementary column operation. Then there exists an $n \times n$ elementary matrix E such that $B = AE$. In fact, E is obtained from I_n by performing the same elementary column operation as that which was performed on A to obtained B.*
Conversely, if E is an $n \times n$ elementary matrix, then AE is the matrix obtained from A by performing the same elementary column operation as that which produces E from I_n.

Briefly, Theorem 3.2 say that $B = AE$, where

$$A \xrightarrow{\text{an elementary column operation}} B$$
$$I_n \xrightarrow{\text{the same elementary column operation}} E.$$

Proof Sketch. We will verify this theorem for each type of elementary column operation.s Recall that for $A \in M_{m\times n}(\mathbb{F})$ and $C = \begin{bmatrix} c_1 & c_2 & \dots & c_n \end{bmatrix} \in M_{n\times n}(\mathbb{F})$, the matrix product AC can be computed as follows

$$AC = \begin{bmatrix} Ac_1 & Ac_2 & \cdots & Ac_n \end{bmatrix}.$$

Suppose $A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \end{bmatrix}$.

1. $a_i \leftrightarrow a_j$. Wlog, assume $i < j$. Then the columns of B are

$$a_1, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots, a_{j-1}, a_i, a_{j+1}, \ldots, a_n.$$

   The columns of E are

$$e_1, \ldots, e_{i-1}, e_j, e_{i+1}, \ldots, e_{j-1}, e_i, e_{j+1}, \ldots, e_n.$$

   Therefore, the columns of AE are

$$Ae_1, \ldots, Ae_{i-1}, Ae_j, Ae_{i+1}, \ldots, Ae_{j-1}, Ae_i, Ae_{j+1}, \ldots, Ae_n,$$

   which are

$$a_1, \ldots, a_{i-1}, a_j, a_{i+1}, \ldots, a_{j-1}, a_i, a_{j+1}, \ldots, a_n.$$

   Therefore, $B = AE$ in this case.

2. See the recorded module for the verification of the remaining elementary column operations and elementary row operations.

□

Theorem 3.3. *Elementary matrices are invertible and the inverse of an elementary matrix is an elementary matrix of the same type.*

Proof Sketch. Suppose A is an elementary matrix obtained from I_m by performing an elementary row operation. We will also verify this theorem for each type of elementary row operations by showing how we can get I_m from A.

1. $R_i \leftrightarrow R_j$. Then I_m is obtained from A by interchanging $R_i \leftrightarrow R_j$.
2. $R_i \leftarrow c * R_i$. Then I_m is obtained from A by $R_i \leftarrow c^{-1} R_i$.
3. $R_i \leftarrow R_i + cR_j$. Then I_m is obtained from A by $R_i \leftarrow R_i - cR_j$.

By previous theorem, there exists an $m \times m$ elementary matrix E such that $I_m = EA$. Therefore, A is invertible. □

3.2 The Rank of a Matrix and Matrix Inverses

Recall: For a linear transformation $T : V \to W$, if $\dim(R(T)) < \infty$, the rank of T is the dimension of the range space of T.

Definition 33. *Let $A \in M_{m\times n}(\mathbb{F})$. We define the rank of the matrix A, denoted $\operatorname{rank}(A)$, to be the rank of the linear transformation $L_A : \mathbb{F}^n \to \mathbb{F}^m, L_A(x) = Ax$, for $x \in \mathbb{F}^n$. That is*

$$\operatorname{rank}(A) = \dim R(L_A) = \dim L_A(\mathbb{F}^n).$$

Example 40. For $n \geq 1$, the ranks of the identity matrix and of the zero matrix are

$$\operatorname{rank}(I_n) = \dim R(I_n) = \dim(\mathbb{F}^n) = n,$$

$$\operatorname{rank}(0_n) = \dim R(0_n) = \dim(\{0\}) = 0.$$

Remark 16.

1. Consider the standard basis $\{e_1, \ldots, e_n\}$ for $\mathbb{F}^n$. We have

$$\begin{aligned} R(L_A) &= \operatorname{span}\{L_A(e_1), L_A(e_2), \ldots, L_A(e_n)\} && \text{(by Theorem 2.3)} \\ &= \operatorname{span}\{Ae_1, Ae_2, \ldots, Ae_n\} && \text{(by Definition of } L_A) \\ &= \operatorname{span}\{a_1, a_2, \ldots, a_n\} && \text{(by Lemma 4)}, \end{aligned}$$

   where $a_j \in \mathbb{F}^m$ is the j-th column of A for $1 \leq j \leq n$. Therefore,

$$\operatorname{rank}(A) = \dim R(L_A) = \dim(\operatorname{span}(\{a_1, a_2, \ldots, a_n\})).$$

   That is, the rank of a matrix is the dimension of the subspace generated by its columns.

2. Since $\{a_1, a_2, \ldots, a_n\}$ generates $R(L_A)$, and any finite spanning set for $R(L_A)$ contains at least $\dim(R(L_A)) = \operatorname{rank}(A)$ vectors, we have $n \geq \operatorname{rank}(A)$.

   Since $R(L_A)$ is a subspace of $\mathbb{F}^m$, $\dim(R(L_A)) \leq \dim(\mathbb{F}^m) = m$. Hence, $\operatorname{rank}(A) \leq m$.

   Therefore, $\operatorname{rank}(A) \leq \min(m, n)$.

Given a matrix A, we want to find the rank of A. If we perform suitable elementary matrix operations on A, we can transform a complicated matrix A to a "simpler" one, where its rank is easier to compute. We will specify what it means by "simpler" matrices later. For now, we want to check whether performing those operations on A changes the rank of the matrix A or not. On the other hand, from Theorems 3.1 and 3.2, the matrix obtained from A after one elementary matrix operation can be written as the matrix multiplication of A with an elementary matrix (from the left or from the right). We will show that the rank of a matrix does not change if we multiply that matrix by an elementary matrix either from the left or from the right. Indeed, we will prove a stronger result which says that the rank of a matrix does not change if we multiply that matrix by an invertible matrix either from the left or from the right or both as long as the matrix multiplications are well-defined. Before proving that theorem, we need the following lemma. The proof of this lemma is left as an exercise.

Lemma 9. *Let $T : V \to W$ be a linear and one-to-one mapping between vector spaces V to a vector space W and V_0 be a subspace of V. Then*

1. *$T(V_0) = \{T(x) \mid x \in V_0\}$ is a subspace of W.*
2. *If $\dim(V_0) < \infty$, then $\dim(V_0) = \dim(T(V_0))$.*

Now we will prove the matrix multiplication from the left and from the right are rank-preserving.

Theorem 3.4. *Let A be an $m \times n$ matrix. If P and Q are invertible $m \times m$ and $n \times n$ matrices, respectively, then*

1. $\operatorname{rank}(AQ) = \operatorname{rank}(A)$.
2. $\operatorname{rank}(PA) = \operatorname{rank}(A)$.
3. $\operatorname{rank}(PAQ) = \operatorname{rank}(A)$.

Proof. 1. Since Q is invertible, L_Q is an isomorphism. Therefore, $L_Q(\mathbb{F}^n) = \mathbb{F}^n$ and

$$L_{AQ}(\mathbb{F}^n) = L_A L_Q(\mathbb{F}^n) = L_A(\mathbb{F}^n).$$

Hence

$$\operatorname{rank}(AQ) = \dim L_{AQ}(\mathbb{F}^n) = \dim L_A(\mathbb{F}^n) = \operatorname{rank}(A).$$

2. Since P is invertible, L_P is an isomorphism. Applying Lemma 9 for $T = L_P, V = W = \mathbb{F}^n$, and $V_0 = L_A(\mathbb{F}^n)$, we have

$$\dim L_A(\mathbb{F}^n) = \dim L_P(L_A(\mathbb{F}^n)),$$

$$\operatorname{rank}(A) = \dim L_{PA}(\mathbb{F}^n),$$

$$\operatorname{rank}(A) = \operatorname{rank}(PA).$$

3. It is obtained from (1) and (2).

□

Next, we will prove two corollaries of Theorem 3.4.

Corollary 3.4.1 (Invertible Matrix Theorem Part 2)**.** Let $A \in M_{n\times n}(\mathbb{F})$. Then A is invertible if and only if $\operatorname{rank}(A) = n$.

Proof. ($\Rightarrow$) Assume A is invertible. Then $I_n = AA^{-1}$. Since A^{-1} is also invertible, by Theorem 3.4,

$$\operatorname{rank}(A) = \operatorname{rank}(AA^{-1}) = \operatorname{rank}(I_n) = n.$$

($\Leftarrow$) Assume $\operatorname{rank}(A) = n$. By definition of rank of a matrix, $n = \dim L_A(\mathbb{F}^n)$. Combining with the fact that $L_A(\mathbb{F}^n)$ is a subspace of $\mathbb{F}^n$, we have $L_A(\mathbb{F}^n) = \mathbb{F}^n$. Thus, L_A is onto. Since for linear mappings from $\mathbb{F}^n$ to itself, onto mappings are one-to-one, and thus are isomorphisms. Therefore, L_A is an isomorphism. Hence, A is invertible. □

Corollary 3.4.2. Elementary row and column operations on a matrix are rank-preserving.

Proof. Suppose $A \in M_{m\times n}(\mathbb{F})$. If B is obtained from A by an elementary row operation, there exists an elementary matrix $E \in M_{m\times m}(\mathbb{F})$ such that $B = EA$. Since E is invertible, by the previous theorem, $\text{rank}(B) = \text{rank}(A)$. Similarly, we can prove that elementary column operations on a matrix are rank-preserving. □

Since elementary matrix operations are rank-preserving, we can apply those operations to transform a complicated matrix to a simpler one, where we can find the rank of the latter matrix easier.

Example 41. Find the rank of the following matrix:

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

Proof. See the recorded module. □

We generalize the process above as follows.

Theorem 3.5. *Let $A \in M_{m\times n}(\mathbb{F})$. Then by means of a finite number of elementary row and column operations, A can be transformed into the matrix*

$$D = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix},$$

where O_1, O_2 and O_3 are zero matrices. Moreover, $r = \text{rank}(A)$.

Proof Sketch. If A is the zero matrix, we're done.
Now suppose $A \neq 0$. Then A has a non-zero entry. By means of at most one elementary row and at most one elementary column (each of type 1), we can move the non-zero entry to the (1,1) position. By means of at most one type-2 operation, we can change that non-zero entry value to 1. By means of at most $(m-1)$ type-3 row operations and at most $(n-1)$ type-3 column operations, we can change all the remaining entries in the first row and in the first column to be 0. Thus after a finite number of elementary matrix operations, we have transformed A to a matrix A' of the form

$$A' = \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right].$$

Using induction hypothesis, we can transform B to the matrix of form D after a finite number of elementary matrix operations. In conclusion, we can transform A into the matrix of form D after a finite number of elementary matrix operations. Since elementary matrix operations preserve the rank, $\text{rank}(A) = \text{rank}(D)$. By Remark 16,

$$\text{rank}(D) = \dim(\text{span}\{e_1, \ldots, e_r, 0, \ldots, 0\}) = \dim(\text{span}\{e_1, \ldots, e_r\}) = r,$$

where $\{e_1, \ldots, e_n\}$ is the standard basis for $\mathbb{F}^n$. Therefore, $\text{rank}(A) = \text{rank}(D) = r$, which completes the proof. □

Note that we can rewrite Theorem 3.5 in terms of matrix products as follows.

Corollary 3.5.1. Let A be an $m \times n$ matrix with $\text{rank}(A) = r$. Then there exist invertible matrices B and C of sizes $m \times m$ and $n \times n$, respectively, such that $D = BAC$, where $D = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix}$ is the $m \times n$ matrix in which O_1, O_2, and O_3 are zero matrices.

Proof. From the previous theorem, we can transform A to D by a finite number of elementary row and column operations. Therefore,

$$D = E_p \cdots E_1 A G_1 G_2 \cdots G_q,$$

where $E_1, \ldots, E_p \in M_{m\times m}(\mathbb{F})$ and $G_1, \ldots, G_q \in M_{n\times n}(\mathbb{F})$ are elementary matrices. Therefore $E_1, \ldots, E_p$ and $G_1, \ldots, G_q$ are invertible. Hence $B = E_p \cdots E_1$ and $C = G_1 G_2 \cdots G_q$ are invertible and $D = BAC$, which completes the proof.

□

We can use Theorem 3.5 to find the rank of a matrix. Specifically, we will apply a series of elementary row and column operations to transfer a complicated matrix A to the matrix D whose top-left corner is an identity matrix I_r and other entries are zero. Then $\text{rank}(A) = r$. However, we can reduce the number of operations by almost a half and still get the rank of a matrix.

Theorem 3.6. *Let $A \in M_{m\times n}(\mathbb{F})$ of rank r. Then by means of a finite number of elementary row and column operations, A can be transformed into the matrix*

$$D_{upper} = \begin{bmatrix} 1 & d_{12} & d_{13} & \cdots & d_{1,r} & d_{1,r+1} & \cdots & d_{1n} \\ 0 & 1 & d_{23} & \cdots & d_{2,r} & d_{2,r+1} & \cdots & d_{2n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & d_{r,r+1} & \cdots & d_{rn} \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Proof Sketch. The proof is almost identical to the proof of Theorem 3.5 except for the step that we need to apply type-3 elementary matrix operations. Suppose $A \neq 0$. We first find a non-zero entry of A. By means of at most one elementary row and at most one elementary column (each of type 1), we can move the non-zero entry to the (1,1) position. By means of at most one type-2 operation, we can change it to 1. By means of at most $(m-1)$ type-3 row operations, we can change all the remaining entries in the first row to be 0. Thus, we have transformed A to a matrix A' of the form

$$A' = \left[\begin{array}{c|ccc} 1 & d_{12} & \cdots & d_{1n} \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right].$$

Using induction hypothesis, we can transform B to the matrix of form D_{upper}. In conclusion, we can transform A into the matrix of form D_{upper}. We have

$$R(D_{upper}) = \dim(\text{span}(\{e_1, d_{12}e_1 + e_2, \ldots, \sum_{i-1}^{r-1} d_{i,r}e_i + e_r, d_{r+1}, \ldots, d_n\}))$$

$$R(D_{upper}) = \dim(\text{span}(\{e_1, e_2, \ldots, e_r, d_{r+1}, \ldots, d_n\}))$$

where $\{e_1, \ldots, e_n\}$ is the standard basis for $\mathbb{F}^n$, d_k is the k-th column of D_{upper} for $1 \leq k \leq n$. Since $d_k = \sum_{i=1}^{r} d_{i,k}e_i$ for $r+1 \leq k \leq n$,

$$\text{span}\{e_1, \ldots, e_r, d_{r+1}, \ldots, d_n\} = \text{span}\{e_1, \ldots, e_r\}.$$

Therefore, $L_{D_{upper}}(\mathbb{F}^n) = \text{span}\{e_1, \ldots, e_r\}$ and

$$\text{rank}(D_{upper}) = \dim(L_{D_{upper}}(\mathbb{F}^n)) = \dim\left(\text{span}\{e_1, \ldots, e_r\}\right) = r.$$

Since elementary matrix operations preserve the rank, $\text{rank}(A) = \text{rank}(D_{upper}) = r$, which completes the proof. □

Remark 17. The proof of Theorem 3.6 suggests a systematic way to transfer a complicated matrix A to the matrix D_{upper}:

- Step 1: Find a non-zero entry of A.
- Step 2: Apply at most one type-1 row operation and at most one type-1 column to move that entry to the (1,1) position.
- Step 3: Apply at most one type-2 row (or column) operation so that the entry at the (1,1) position is $1_{\mathbb{F}}$.
- Step 4: Apply at most $(m-1)$ type-3 elementary row operations so that all the remaining entries in the first row to be 0. The updated matrix is now of the form

$$\left[\begin{array}{c|ccc} 1 & d_{12} & \cdots & d_{1n} \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right].$$

- Step 5: Repeat Steps 1,2,3,4 for the matrix B. Continue this process till we get a matrix whose form is like D_{upper}.
- Step 6: Then $\text{rank}(A) = r =$ the number of nonzero rows of D_{upper}.

Example 42. Find the rank of the following matrix:

$$A = \begin{pmatrix} 1 & -1 & -3 & 1 & 0 \\ -2 & 1 & 4 & -1 & 3 \\ 3 & -1 & -5 & 1 & -6 \end{pmatrix}$$

Proof. See the recorded module. □

Next, we will use the definition of matrix ranks and Corollary 3.5.1 to prove many interesting results about rank of a matrix.

Corollary 3.6.1. Let A be an $m \times n$ matrix. Then

1. $\text{rank}(A^t) = \text{rank}(A)$.
2. $\text{rank}(A)$ = the dimension of the subspace generated by the columns of A = the dimension of the subspace generated by the rows of A.

Proof. 1. From Corollary 3.5.1, there exists invertible matrices B and C such that $D = BAC$. Then

$$D^t = (BAC)^t = C^t A^t B^t.$$

Since B and C are invertible, B^t and C^t are invertible (by Lemma 8). Therefore,

$$\text{rank}(A^t) = \text{rank}(D^t).$$

Since D^t is an $n \times m$ matrix with the form of the matrix D in Corollary 3.5.1, $\text{rank}(D^t) = r$, where $r = \text{rank}(A)$. Therefore,

$$\text{rank}(A^t) = \text{rank}(D^t) = r = \text{rank}(A).$$

2. In Remark 16, we proved that $\text{rank}(A)$ is the dimension of the subspace generated by the columns of A. Applying Remark 16 for the matrix A^t, we have $\text{rank}(A^t)$ is the dimension of the subspace generated by the columns of A^t. Since the columns of A^t are the rows of A, $\text{rank}(A^t)$ is the dimension of the subspace generated by the rows of A. Combining with part 1, we have the conclusion.

□

Theorem 3.7. *Let A and B be matrices such that the product AB is defined. Then*

$$\text{rank}(AB) \leq \min\{\text{rank}(A), \text{rank}(B)\}.$$

Proof. Suppose $A \in M_{m\times n}(\mathbb{F})$ and $B \in M_{n\times p}(\mathbb{F})$. Since

$$R(L_{AB}) = \{ABx \mid x \in \mathbb{F}^p\} \subset \{Ay \mid y \in \mathbb{F}^n\} = R(L_A),$$

we have

$$\text{rank}(AB) = \dim R(L_{AB}) \leq \dim R(L_A) = \text{rank}(A).$$

On the other hand,

$$\text{rank}(AB) = \text{rank}((AB)^T) = \text{rank}(B^T A^T) \leq \text{rank}(B^T) = \text{rank}(B).$$

So $\text{rank}(AB) \leq \min\{\text{rank}(A), \text{rank}(B)\}$. □

The previous theorem explains one of the question that we discussed last time. If $A \in M_{3\times 2}(\mathbb{F})$ and $B \in M_{2\times 3}(\mathbb{F})$, then $\text{rank}(AB) \leq \min\{\text{rank}(A), \text{rank}(B)\} \leq \min\{2, 3\} = 2$. Therefore, $AB \in M_{3\times 3}(\mathbb{F})$ is not invertible. Below is another fun question.

Question: Given $A \in M_{m\times n}(\mathbb{F}), B \in M_{n\times m}(\mathbb{F})$. We know that, in general, $AB \neq BA$. What about $\text{rank}(AB)$ and $\text{rank}(BA)$? Is $\text{rank}(AB) = \text{rank}(BA)$? Prove or disprove.

3.3 Four Fundamental Subspaces of a Matrix

From a matrix $A \in M_{m\times n}(\mathbb{F})$ we can define the following vector spaces.

Definition 34. *Let $A \in M_{m\times n}(\mathbb{F})$. Define*

$$\begin{aligned}
\mathrm{Col}(A) &:= \{Ax \mid x \in \mathbb{F}^n\} \\
&= \{\textit{all linear combinations of columns of } A\} \\
&= \mathrm{span}\{\textit{columns of } A\}, \ \textit{called the column space of } A, \\
\mathrm{Row}(A) &:= \mathrm{Col}(A^T) = \{A^T y \mid y \in \mathbb{F}^m\} \\
&= \{\textit{all linear combinations of rows of } A\} \\
&= \mathrm{span}\{\textit{rows of } A\} \ \textit{called the row space of } A, \\
Null(A) &:= \{x \in \mathbb{F}^n \mid Ax = 0\}, \ \textit{called the null space of } A, \\
Null(A^T) &:= \{y \in \mathbb{F}^m \mid A^T y = 0\}, \ \textit{called the left null space of } A.
\end{aligned}$$

Denote $\mathrm{nullity}(A) := \dim Null(A)$.

Theorem 3.8. *Let $A \in M_{m\times n}(\mathbb{F})$. Then*

1. $\mathrm{Col}(A)$ *and* $Null(A^T)$ *are subspaces of* $\mathbb{F}^m$; $\mathrm{Row}(A)$ *and* $Null(A)$ *are subspaces of* $\mathbb{F}^n$.
2. $\mathrm{rank}(A) = \dim \mathrm{Col}(A) = \dim \mathrm{Row}(A)$.
3. $\mathrm{nullity}(A^T) = m - \mathrm{rank}(A)$ *and* $\mathrm{nullity}(A) = n - \mathrm{rank}(A)$.
4. *If* $\mathbb{F} = \mathbb{R}$, $A \in M_{m\times n}(\mathbb{R})$ *and* $\mathbb{R}^m = \mathrm{Col}(A) \oplus Null(A^T)$ *and* $\mathbb{R}^n = \mathrm{Row}(A) \oplus Null(A)$.

Proof. Here are the proofs of some parts.
(3). The Rank-Nullity Theorem for $L_A : \mathbb{F}^n \to \mathbb{F}^m$ implies that

$$\dim \mathbb{F}^n = \dim R(L_A) + \dim N(L_A) = \mathrm{rank}(A) + \mathrm{nullity}(A).$$

Applying the rank-nullity theorem for L_{A^t}, we have

$$\dim \mathbb{F}^m = \dim R(L_{A^t}) + \dim N(L_{A^t}) = \mathrm{rank}(A) + \mathrm{nullity}(A^t).$$

(4). First prove that $\mathrm{Row}(A) \cap Null(A) = \{0\}$ (prove this). Therefore, the direct sum of $\mathrm{Row}(A)$ and $Null(A)$ is well-defined. By Theorem 1.12, we have

$$\dim(\mathrm{Row}(A)+Null(A)) = \dim \mathrm{Row}(A)+\dim Null(A)-\dim(\mathrm{Row}(A) \cap Null(A)) = \dim \mathrm{Row}(A)+\mathrm{nullity}(A).$$

By Corollary 3.6.1, $\mathrm{rank}(A) = \dim \mathrm{Row}(A)$. Therefore

$$\dim(\mathrm{Row}(A) + Null(A)) = \mathrm{rank}(A) + \mathrm{nullity}(A) = n = \dim \mathbb{F}^n.$$

Since the sum $\mathrm{Row}(A) + Null(A)$ is a subspace of $\mathbb{F}^n$ and $\dim(\mathrm{Row}(A) + Null(A)) = \dim \mathbb{F}^n$, we have

$$\mathrm{Row}(A) + Null(A) = \mathbb{F}^n.$$

Combining with $\mathrm{Row}(A) \cap Null(A) = \{0\}$, we conclude that

$$\mathrm{Row}(A) \oplus Null(A) = \mathbb{F}^n.$$

□

3.4 The Inverse of a Matrix

Theorem 3.9 (Invertible Matrix Theorem Parts 3)**.** *Let $A \in M_{n\times n}(\mathbb{F})$. Then the following statements are equivalent.*

1. *A is invertible.*
2. *The columns of A form a basis for $\mathbb{F}^n$.*
3. *The rows of A form a basis for $\mathbb{F}^n$.*
4. *A is a product of elementary matrices.*

Proof. We will prove (2), (3), (4) is equivalent to (1).
(2) $\Leftrightarrow$ (1): $\text{rank}(A) = n \Leftrightarrow \dim(\text{Col}(A)) = n \xLeftrightarrow{\text{since } A \text{ has } n \text{ columns}}$ the columns of A form a basis for $\mathbb{F}^n$. Similarly, we can prove (1) $\Leftrightarrow$ (3).
(4) $\Rightarrow$ (1) Suppose A is a product of elementary matrices $A = E_1E_2 \dots E_p$. Since elementary matrices are invertible and the matrix product of invertible matrices is invertible, we conclude that A is invertible and

$$A^{-1} = E_p^{-1} \dots E_2^{-1}E_1^{-1}.$$

(1) $\Rightarrow$ (4) We have $D = BAC$ where $D = \begin{bmatrix} I_r & O_1 \\ O_2 & O_3 \end{bmatrix}$, $r = \text{rank}(A)$, and B and C are products of elementary matrices. Since A is invertible, $r = n$ and $D = I_n$. Therefore, $A = B^{-1}I_nC^{-1} = B^{-1}C^{-1}$. Moreover, since B and C are products of elementary matrices and the inverse of an elementary matrix is an elementary matrix, A is the product of elementary matrix. □

Now, we will present a simple method to compute the inverse of a matrix that utilizes elementary **row** operations.

Theorem 3.10. *1. If A is an invertible $n \times n$ matrix, it is possible to transform $(A \mid I_n)$ into the matrix $(I_n \mid A^{-1})$ by means of a finite number of elementary* **row** *operations.*

2. *Conversely, suppose A is an $n \times n$ matrix and there exists an $n \times n$ matrix B such that $(A \mid I_n) \rightsquigarrow (I_n \mid B)$ via a finite number of elementary row operations, then A is invertible and $B = A^{-1}$.*

Proof. 1. Since $AM = (Av_1\ Av_2\ \cdots Av_p)$ for any $M = (v_1\ v_2\ \cdots v_p) \in M_{n\times p}(\mathbb{F})$, we have

$$A^{-1}(A \mid I_n) = (A^{-1}A \mid A^{-1}I_n) = (I_n \mid A^{-1}).$$

By the invertible matrix theorem, since A^{-1} is invertible, A^{-1} is a product of elementary matrices

$$A^{-1} = E_p \dots E_1.$$

Therefore, we have

$$E_pE_{p-1} \dots E_1(A \mid I_n) = (I_n \mid A^{-1}).$$

On the other hand, $E_pE_{p-1}\dots E_1(A \mid I_n)$ is the matrix obtained from $(A \mid I_n)$ by applying consecutively p elementary row operations associated with the elementary matrices $E_1, \dots, E_p$:

$$(A \mid I_n) \xrightarrow{\text{an elementary row operation}} E_1(A \mid I_n) \xrightarrow{\text{an elementary row operation}} E_2E_1(A \mid I_n) \to \cdots$$
$$\cdots \xrightarrow{\text{an elementary row operation}} E_pE_{p-1}\dots E_1(A \mid I_n).$$

In conclusion, after those p elementary row operations, $(A \mid I_n)$ is transformed to $(I_n \mid A)$.

2. Let $G_1, \dots, G_q$ be elementary matrices associated with the elementary row operations that transform $(A \mid I_n) \rightsquigarrow (I_n \mid B)$. Then, we have

$$G_q \dots G_1(A \mid I_n) = (I_n \mid B).$$

Let $G = G_q \dots G_1$ then $(GA \mid G) = (I_n \mid B)$. So $GA = I_n$ and $B = G$. So $BA = I_n$. By the invertible matrix theorem, $B = A^{-1}$. □

Remark 18. Theorem 3.10 suggests an algorithm to check whether a square matrix is invertible or not and how to find A^{-1}. It is called the Gauss-Jordan method to find the inverse of a square matrix (if exists).

- Step 1: If the first column of A is a zero vector, A is not invertible by the Invertible Matrix Theorem. Otherwise, the first row of A has a non-zero entry.
- Step 2: By means of at most one type-1 and one type-2 elementary row operation $(A \mid I_n)$, we can move that non-zero entry to the (1,1)-position and its new value is 1.
- Step 3: By means of at most (n-1) type-3 row operations, we can change all the remaining entries in the first row to be 0. Thus, we have transformed $(A \mid I_n)$ to a matrix of the form

$$\left[\begin{array}{c|ccc} 1 & d_{12} & \cdots & d_{1,2n} \\ \hline 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{array}\right].$$

- Step 4: Repeat Steps 1,2,3 for matrix Q. If the first column of Q is a zero vector, A is not invertible and we stop the procedure. Otherwise, continue this process until we get the matrix

$$C' = \begin{bmatrix} 1 & d_{12} & \cdots & d_{1,n} & d_{1,n+1} & \cdots & d_{1,2n} \\ 0 & 1 & \cdots & d_{2,n} & d_{2,n+1} & \cdots & d_{2,2n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & d_{n,n+1} & \cdots & d_{n,2n} \end{bmatrix}.$$

Note that from Step 1 to Step 4, we go all the way forward to transform $(A \mid I_n)$ to a matrix where the entries below the main diagonal are all zeros, $C'_{ij} = 0$ for all $1 \le j < i \le n$ and $C'_{ii} = 0$ for $i = 1, \dots n$. For the remaining steps, we go all the way backward to produce zeros above the main diagonal.

- Step 5: By means of at most $(n-1)$ type-3 row operations, we can transfer all entries at the n-th column of C' are zero except the last entry and $C' \rightsquigarrow C_n$:

$$C_n = \begin{bmatrix} 1 & d_{12} & \cdots & 0 & d_{1,n+1} & \cdots & d_{1,2n} \\ 0 & 1 & \cdots & 0 & d_{2,n+1} & \cdots & d_{2,2n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & d_{n,n+1} & \cdots & d_{n,2n} \end{bmatrix}.$$

- Step 6: By means of at most $(n-2)$ type-3 row operations, we can transfer all entries at the $(n-1)$ column of C_n are zeros except at the (n-1,n-1)-position and $C_n \rightsquigarrow C_{n-1}$.

- Step 7: Continue this process until we get the matrix of the form $(I_n \mid B)$. Then B is the inverse of A.

Example 43. Find the inverse (if exists) of $A = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 2 \end{bmatrix}$.

Proof. See the recorded module. □

Example 44. Find the inverse (if exists) of $A = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \\ 3 & 6 & 2 \end{bmatrix}$.

Proof. See the recorded module. □

3.5 Systems of Linear Equations

Definition 35. • *The system of equations*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned} \tag{3}$$

where $a_{ij}, b_i \in \mathbb{F}$ $(1 \le i \le m, 1 \le j \le n)$ and $x_1, x_2, \ldots, x_n$ are n variables taking values in $\mathbb{F}$, is called a system of m linear equations in n unknowns over the field $\mathbb{F}$. Note that the system (3) can be written as a matrix product $Ax = b$, where

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}, \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, \quad \text{and} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}.$$

- *The matrix A is called the coefficient matrix of the system (3).*
- *The $m \times (n+1)$ matrix $(A \mid b)$ is called the augmented matrix of the system $Ax = b$.*
- *A solution to the system (3) is an n-tuple $c = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} \in \mathbb{F}^n$ such that $Ac = b$.*
- *The set of all solutions to the system (3) is called the solution set of the system.*
- *The system (3) is called consistent if its solution set is nonempty.*
- *The system (3) is called inconsistent if its solution set is empty.*
- *A system $Ax = b$ of m linear equations in n unknowns is said to be homogeneous if $b = 0$. Otherwise, the system is said to be inhomogeneous.*

Theorem 3.11. *Let $A \in M_{m\times n}(\mathbb{F})$ and consider $Ax = 0$. Then the set K_H of all solutions to $Ax = 0$ is a subspace of $\mathbb{F}^n$ and*

$$\dim K_H = n - \operatorname{rank}(A).$$

Proof. Observe that $K_H = N(L_A) = Null(A)$. Therefore, K_H is a subspace of $\mathbb{F}^n$.
Applying the Rank-Nullity theorem for $L_A : \mathbb{F}^n \to \mathbb{F}^m$, we have

$$n = \dim R(L_A) + \dim Null(A) = \operatorname{rank}(A) + \dim K_H.$$

So $\dim K_H = n - \operatorname{rank}(A)$. □

Remark 19. Let K_H be the solution set to $Ax = 0$. Then

1. $K_H \neq \emptyset$. Indeed, $0 \in K_H$ is the trivial solution of $Ax = 0$.
2. $K_H = \{0\}$ if and only if $\operatorname{rank} A = n$. In this case, we say the matrix A is of full column rank.
3. If $m < n$, then $\operatorname{rank} A \leq m < n$ by Theorem 3.7, so the system $Ax = 0$ has a nonzero solution. In words, a homogeneous system of linear equations with more unknowns than number of equations has a nonzero solution.

Theorem 3.12. *Given $A \in M_{m\times n}(\mathbb{F})$ and $b \in \mathbb{F}^m$. Let*

$$K = \{x \in \mathbb{F}^n \mid Ax = b\} \quad \text{and} \quad K_H = \{x \in \mathbb{F}^n \mid Ax = 0\}.$$

Then for any solution c to $Ax = b$, we have

$$K = c + K_H = \{c + k \mid k \in K_H\}.$$

Hence if $Ax = b$ is consistent, then its solution set is a coset of K_H.

Proof. In the recorded modules. □

Theorem 3.13 (Invertible Matrix Theorem - Part 4)**.** *Let A be an $n \times n$ matrix. Then the following are equivalent:*

1. *A is invertible.*
2. *For some $b \in \mathbb{F}^m$, the equation $Ax = b$ has a unique solution.*
3. *For every $b \in \mathbb{F}^m$, the equation $Ax = b$ has a unique solution.*

Proof. $(1 \Rightarrow 3)$ Suppose A is invertible. Let $b \in \mathbb{F}^m$ be given. Clearly $x = A^{-1}b$ is one solution to $Ax = b$, since $A(A^{-1}b) = I_n b = b$. Conversely, from $Ax = b$ we can deduce

$$A^{-1}b = A^{-1}(Ax) = I_n x = x.$$

That is, if x is a solution, then $x = A^{-1}b$. Hence the system $Ax = b$ has a unique solution $x = A^{-1}b$.
$(3 \Rightarrow 2)$ is obvious.
$(2 \Leftarrow 1)$ Suppose the equation $Ax = b$ has a unique solution c. Let K_H be the solution set of $Ax = 0$. By Theorem 3.12, $\{c\} = c + K_H$. So $K_H = \{0\}$. By Theorem 3.11, $0 = \dim K_H = n - \operatorname{rank}(A)$. Therefore, $\operatorname{rank} A = n$, which implies A is invertible. □

Exercise: Let $A \in M_{m\times n}(\mathbb{F})$ and $B \in M_{n\times m}(\mathbb{F})$. Prove that if $I_m + AB$ is invertible then $I_n + BA$ is invertible.

Theorem 3.14. *Let $Ax = b$ be a system of linear equations. Then the system is consistent if and only if* $\operatorname{rank}(A) = \operatorname{rank}(A \mid b)$.

Proof.

$$\begin{aligned} Ax = b \text{ has a solution} &\Leftrightarrow b \in R(L_A) \\ &\Leftrightarrow b \in \operatorname{span}\{Col_1(A), \ldots, Col_n(A)\} \\ &\Leftrightarrow \operatorname{span}\{Col_1(A), \ldots, Col_n(A)\} = \operatorname{span}\{Col_1(A), \ldots, Col_n(A), b\} \\ &\Leftrightarrow \dim \operatorname{span}\{Col_1(A), \ldots, Col_n(A)\} = \dim \operatorname{span}\{Col_1(A), \ldots, Col_n(A), b\} \\ &\Leftrightarrow \operatorname{rank}(A) = \operatorname{rank}(A \mid b). \end{aligned}$$

□

Definition 36. *Two systems of linear equations are called equivalent if they have the same solution set.*

Theorem 3.15. *Let $Ax = b$ be a system of m linear equations in n unknowns and let C be an $m \times m$ invertible matrix. Then the system $(CA)x = Cb$ is equivalent to $Ax = b$.*

Proof. In the recorded modules. □

Corollary 3.15.1. Let $Ax = b$ be a system of m linear equations in n unknowns. If $(A' \mid b')$ is obtained from $(A \mid b)$ by a finite number of elementary row operations, then the system $A'x = b'$ is equivalent to the original system.

Now, we will describe a method for solving any system of linear equations by transforming the augmented matrix to the reduced row echelon form.

Definition 37. *A matrix is said to be in reduced row echelon form (RREF) if the following four conditions are satisfied.*

1. *Nonzero rows (if any) are at the top of the matrix. Zero rows (if any) are at the bottom.*
2. *The first nonzero entry in each nonzero row is 1, called a leading one.*
3. *The leading one in a nonzero row is the only nonzero entry in its column.*
4. *The leading one in each nonzero row is to the right of the leading one in any row above it.*

Examples of matrices in RREF:

$$\begin{bmatrix} 1 & 0 & 0 & 2 & -1 & 6 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 & -3 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 & 2 & 0 & -2 & 3 \\ 0 & 1 & -1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Examples of matrices not in RREF:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Example 45. Determine which of the following matrices are in RREF.

$$(a)\ \begin{bmatrix}1&0&3&0\\0&1&1&0\\0&0&0&1\end{bmatrix}\quad (b)\ \begin{bmatrix}1&0&0&3\\0&1&1&1\\0&0&1&1\end{bmatrix}\quad (c)\ \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\end{bmatrix}\quad (d)\ \begin{bmatrix}1&0&1&0&1\\0&1&0&0&2\\0&0&0&1&3\end{bmatrix}$$

Every matrix can be transformed to a matrix in RREF via a sequence of elementary row operations. We call such a transformation a *row reduction*. Here is a description of one algorithm for row reducing a matrix to RREF. In addition to describing the general steps, we will illustrate them by applying them to the matrix

$$A=\begin{bmatrix}2&4&1&0&-4&2\\0&0&2&-4&4&4\\1&2&2&-3&1&4\\3&6&-2&7&-13&4\end{bmatrix}$$

Gaussian Elimination to Row Reduce a Nonzero Matrix into RREF

1. In the leftmost nonzero column, use elementary row operations (if necessary) to get a 1 in the first row. (This will be a leading one.)

$$A=\begin{bmatrix}2&4&1&0&-4&2\\0&0&2&-4&4&4\\1&2&2&-3&1&4\\3&6&-2&7&-13&4\end{bmatrix}\xrightarrow{R_1*\frac{1}{2}}\begin{bmatrix}1&2&\frac{1}{2}&0&-2&1\\0&0&2&-4&4&4\\1&2&2&-3&1&4\\3&6&-2&7&-13&4\end{bmatrix}$$

2. By means of type 3 elementary row operations, use the first row to create zeros in the remaining entries of the leftmost nonzero column; that is, <u>below</u> the leading one created in the previous step.

$$\begin{bmatrix}1&2&\frac{1}{2}&0&-2&1\\0&0&2&-4&4&4\\1&2&2&-3&1&4\\3&6&-2&7&-13&4\end{bmatrix}\begin{matrix}\\\\\xrightarrow{R_3\leftarrow R_3-R_1}\\\xrightarrow{R_4\leftarrow R_4-3*R_1}\end{matrix}\begin{bmatrix}1&2&\frac{1}{2}&0&-2&1\\0&0&2&-4&4&4\\0&0&\frac{3}{2}&-3&3&3\\0&0&-\frac{7}{2}&7&-7&1\end{bmatrix}$$

3. Consider the submatrix consisting of the columns to the right of the column we just modified and the rows beneath the row that just got a leading one. Use elementary row operations (if necessary) to get a leading one in the top of the first nonzero column of this submatrix.

$$\left[\begin{array}{c|cccc}1&2&\frac{1}{2}&0&-2&1\\\hline0&0&2&-4&4&4\\0&0&\frac{3}{2}&-3&3&3\\0&0&-\frac{7}{2}&7&-7&1\end{array}\right]\xrightarrow{R_2*\frac{1}{2}}\left[\begin{array}{c|cccc}1&2&\frac{1}{2}&0&-2&1\\\hline0&0&1&-2&2&2\\0&0&\frac{3}{2}&-3&3&3\\0&0&-\frac{7}{2}&7&-7&1\end{array}\right]$$

4. Use elementary row operations to obtain zeros <u>below</u> the 1 created in the preceding step. (But do not create zeroes above the leading one now; Gaussian elimination does this later.)

$$\begin{bmatrix} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & \frac{3}{2} & -3 & 3 & 3 \\ 0 & 0 & -\frac{7}{2} & 7 & -7 & 1 \end{bmatrix} \xrightarrow[R_4 \leftarrow R_4 + \frac{7}{2} * R_2]{R_3 \leftarrow R_3 - \frac{3}{2} * R_2} \begin{bmatrix} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 \end{bmatrix}$$

5. Repeat Steps 3 and 4 until no nonzero rows remain. This completes the *forward phase.*

$$\left[\begin{array}{cccccc} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 8 \end{array}\right] \xrightarrow{R_3 \leftrightarrow R_4} \left[\begin{array}{cccccc} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \xrightarrow{R_3 \leftarrow \frac{1}{8} * R_3} \left[\begin{array}{cccccc} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

6. Now we will create zeroes above the leading ones. Working backwards, begin with the last nonzero row and add multiples of it to each row above it to create zeros above its leading one.

$$\begin{bmatrix} 1 & 2 & \frac{1}{2} & 0 & -2 & 1 \\ 0 & 0 & 1 & -2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[R_2 \leftarrow R_2 - 2 * R_3]{R_1 \leftarrow R_1 - R_3} \begin{bmatrix} 1 & 2 & \frac{1}{2} & 0 & -2 & 0 \\ 0 & 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

7. Repeat the process in Step 6 for the second-to-last nonzero row, then the third-to-last nonzero row, etc. until it has been performed to every nonzero row except the first row. This completes the *backward phase.* At this point the matrix should be in RREF.

$$\begin{bmatrix} 1 & 2 & \frac{1}{2} & 0 & -2 & 0 \\ 0 & 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{R_1 \leftarrow R_1 - \frac{1}{2} * R_2} \begin{bmatrix} 1 & 2 & 0 & 1 & -3 & 0 \\ 0 & 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ in RREF.}$$

We have the following conclusion.

Theorem 3.16. *Gaussian elimination transforms any matrix into an RREF matrix.*

Notes.

1. Gaussian elimination is not the only way to transform a matrix to RREF. For example, you could just do a forward phase, creating zeroes below <u>and above</u> each leading one at the same time. Then there is no need for the backward phase. (This method is called Gauss-Jordan elimination.)

2. Guassian elimination is *non-deterministic*. This means that you have choices when you execute this algorithm. For example, in the example illustrating Gaussian elimination, at step 1 (using elementary row operations to get a 1 in the top row, first nonzero column), we could have used

$$A = \begin{bmatrix} 2 & 4 & 1 & 0 & -4 & 2 \\ 0 & 0 & 2 & -4 & 4 & 4 \\ 1 & 2 & 2 & -3 & 1 & 4 \\ 3 & 6 & -2 & 7 & -13 & 4 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{bmatrix} 1 & 2 & 2 & -3 & 1 & 4 \\ 0 & 0 & 2 & -4 & 4 & 4 \\ 2 & 4 & 1 & 0 & -4 & 2 \\ 3 & 6 & -2 & 7 & -13 & 4 \end{bmatrix}$$

This will change the next steps of the calculation; in particular, step 2 will not introduce any annoying fractions in the third column. When executing Gaussian elimination, you have the freedom to choose how to accomplish step 1 and each iteration of step 3, and some choices may yield easier calculations.

Now we explore how RREFs can be helpful in solving systems of linear equations.

Definition 38. *Let B be the RREF of a coefficient matrix of a system of linear equations $Ax = b$. If the j-th column of B does not contain a leading one, then we call x_j a free variable.*

Remark 20. Let B be the RREF of the coefficient matrix of the system $Ax = b$, where $A \in M_{m\times n}(\mathbb{F})$ and $b \in \mathbb{F}^m$. Then

1. $\operatorname{rank}(A) = \operatorname{rank}(B)$ = number of leading ones of B = number of nonzero rows of B.
2. Number of free variables = n − number of leading ones = $n - \operatorname{rank}(A)$.

Proof. 1. Since B is obtained from A via a finite number of elementary row operations, we have $\operatorname{rank}(A) = \operatorname{rank}(B)$. On the other hand, by the definition of RREF, the nonzero rows of B are linearly independent. So the nonzero rows of B form a basis for $\operatorname{Row}(B)$. Therefore, $\operatorname{rank}(B) = \dim \operatorname{Row}(B)$ = number of nonzero rows of B = number of leading ones of B. We get (2) from (1). □

Algorithm for Solving a System of Linear Equations $Ax = b$, where $A \in M_{m\times n}(\mathbb{F})$ and $b \in \mathbb{F}^m$
Here are the general steps. Each step is illustrated for the following example (the field is $\mathbb{Q}$):

$$\begin{array}{rcrcrcrcrcr} x_1 & + & 2x_2 & & & - & x_4 & + & 7x_5 & = & -4 \\ 3x_1 & + & x_2 & + & 5x_3 & & & - & 5x_5 & = & -2 \\ x_1 & & & + & 2x_3 & + & x_4 & - & 5x_5 & = & 4 \\ & & x_2 & - & x_3 & + & x_4 & + & 2x_5 & = & 6 \end{array}$$

1. Write the augmented matrix for the system.

$$(A \mid b) = \left[\begin{array}{rrrrr|r} 1 & 2 & 0 & -1 & 7 & -4 \\ 3 & 1 & 5 & 0 & -5 & -2 \\ 1 & 0 & 2 & 1 & -5 & 4 \\ 0 & 1 & -1 & 1 & 2 & 6 \end{array}\right]$$

2. Use elementary row operations to transform the augmented matrix into RREF $(A' \mid b')$.

$$(A' \mid b') = \left[\begin{array}{ccccc|c} 1 & 0 & 2 & 0 & -3 & -1 \\ 0 & 1 & -1 & 0 & 4 & 1 \\ 0 & 0 & 0 & 1 & -2 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

3. Write the system of linear equations corresponding to the RREF.

$$\begin{array}{rcrcrcrcr} x_1 & & + & 2x_3 & & - & 3x_5 & = & -1 \\ & x_2 & - & x_3 & & + & 4x_5 & = & 1 \\ & & & & x_4 & - & 2x_5 & = & 5 \\ & & & & & & 0 & = & 0 \end{array}$$

4. If the system contains an equation of the form $0 = 1$, then stop as the system is inconsistent.

5. Otherwise, assign parametric values $t_1, t_2, \ldots, t_{n-r}$ to the free variables and then solve the remaining variables in terms of the free variables. Here r is the number of nonzero rows of A'.

   - The free variables in the example are x_3 and x_5. Let $x_3 = t_1 \in \mathbb{Q}$ and $x_5 = t_2 \in \mathbb{Q}$.
   - Then the remaining variables can be expressed as

$$\begin{aligned} x_1 &= -1 - 2t_1 + 3t_2 \\ x_2 &= 1 + t_1 - 4t_2 \\ x_4 &= 5 + 2t_2. \end{aligned}$$

6. Reorganize the equations from the previous step (i.e., the equations expressing the variables in terms of the parameters) as a vector equation in the form

$$x = x_0 + t_1 u_1 + \cdots + t_{n-r} u_{n-r},$$

   where $x_0, u_1, \ldots, u_{n-r}$ are specific vectors in $\mathbb{F}^n$.

   - In the example, the equations for all 5 variables can be displayed as follows:

$$\begin{array}{rcrcrcr} x_1 & = & -1 & - & 2t_1 & + & 3t_2 \\ x_2 & = & 1 & + & t_1 & - & 4t_2 \\ x_3 & = & 0 & + & t_1 & & \\ x_4 & = & 5 & & & + & 2t_2 \\ x_5 & = & 0 & & & + & t_2 \end{array}$$

     From this we can read off "by inspection" the vector equation

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 0 \\ 5 \\ 0 \end{bmatrix} + t_1 \begin{bmatrix} -2 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t_2 \begin{bmatrix} 3 \\ -4 \\ 0 \\ 2 \\ 1 \end{bmatrix}.$$

7. Then the solutions to $Ax = b$ are all the vectors $x \in \mathbb{F}^n$ of the form

$$x = x_0 + t_1u_1 + \cdots + t_{n-r}u_{n-r}, \qquad (t_1, \ldots, t_{n-r} \in \mathbb{F}).$$

(This form of describing the solutions is sometimes called *parametric form.*) The solution set K to $Ax = b$ is the coset $K = x_0 + \text{span}(u_1, \ldots, u_{n-r})$.

- In the example, we let $x_0 = (-1, 1, 0, 5, 0)^T$, $u_1 = (-2, 1, 1, 0, 0)$, and $u_2 = (3, -4, 0, 2, 1)^T$. Then the solutions to $Ax = b$ are described in parametric form by

$$x = x_0 + t_1u_1 + t_2u_2 \quad \text{where } t_1, t_2 \text{ vary over } \mathbb{Q}.$$

The solution set is the coset $x_0 + \text{span}(u_1, u_2) \subseteq \mathbb{Q}^5$.

Example 46. Express the solution set for the following system in parametric form.

$$\begin{array}{rcrcrcl} x_1 & & & + & x_3 & + & 2x_4 = 4 \\ 2x_1 & + & x_2 & + & 4x_3 & + & x_4 = 6 \\ -x_1 & - & 4x_2 & - & 9x_3 & + & 5x_4 = 4 \end{array}$$

Solution.

$$\left[\begin{array}{cccc|c} 1 & 0 & 1 & 2 & 4 \\ 2 & 1 & 4 & 1 & 6 \\ -1 & -4 & -9 & 5 & 4 \end{array}\right] \begin{array}{l} \\ \xrightarrow{R_2-2R_1} \\ \xrightarrow{R_3+R_1} \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 1 & 2 & 4 \\ 0 & 1 & 2 & -3 & -2 \\ 0 & -4 & -8 & 7 & 8 \end{array}\right] \xrightarrow{R_3+4R_2}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 1 & 2 & 4 \\ 0 & 1 & 2 & -3 & -2 \\ 0 & 0 & 0 & -5 & 0 \end{array}\right] \xrightarrow{-\frac{1}{5}R_3} \left[\begin{array}{cccc|c} 1 & 0 & 1 & 2 & 4 \\ 0 & 1 & 2 & -3 & -2 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} \xrightarrow{R_1-2R_3} \\ \xrightarrow{R_2+3R_3} \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 4 \\ 0 & 1 & 2 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

The corresponding system of equations is

$$\begin{array}{rcrcrcl} x_1 & & & + & x_3 & = & 4 \\ & & x_2 & + & 2x_3 & = & -2 \\ & & & & x_4 & = & 0 \end{array}$$

The free variable is x_3. Let $x_3 = s$. The other equations can be expressed in terms of s as follows:

$$\begin{aligned} x_1 &= 4 - s \\ x_2 &= -2 - 2s \\ x_4 &= 0. \end{aligned}$$

The general solution to the system, expressed in parametric form, is

$$x = \begin{bmatrix} 4 - s \\ -2 - 2s \\ s \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ -2 \\ 0 \\ 0 \end{bmatrix} + s \begin{bmatrix} -1 \\ 2 \\ 1 \\ 0 \end{bmatrix}, \quad s \in \mathbb{F}.$$

Remark 21.

- Of all methods for transforming a matrix into its RREF, Gaussian elimination requires the fewest arithmetic operations. Indeed, for large matrices, it requires approximately 50% fewer operations than the Gaussian-Jordan elimination, where the matrix is transformed to RREF by using the first nonzero entry in each row to make all other entries of that column to be 0. Therefore, Gaussian elimination is a preferred method when solving systems of linear equations on a computer.
- There are other methods to solve systems of linear equations using matrix decompositions such as LU-decomposition, QR-decomposition,...

Theorem 3.17. *Let $[A \mid b]$ be a consistent system of m linear equations in n variables. Suppose the RREF of $(A \mid b)$ has r nonzero rows. If the general solution to $Ax = b$ obtained by the procedure above is of the form*

$$x = x_0 + t_1 u_1 + \cdots + t_{n-r} u_{n-r}, \qquad (t_1, \ldots, t_{n-r} \in \mathbb{F})$$

then $x_0 \in \mathbb{F}^n$ is a solution to $Ax = b$ and $\{u_1, \ldots, u_{n-r}\}$ is a basis for the solution set of the correponding homogeneous sytem.

Proof. Let $K = \{x \in \mathbb{F}^n \mid Ax = b\}$ and $K_H = \{x \in \mathbb{F}^n \mid Ax = 0\}$. We have $r = \text{rank}(A)$ from Remark 14.

- Choose $t_1 = \ldots = t_{n-r} = 0$, we get $x_0 \in K$.
- So $K = x_0 + K_H$ by Theorem 3.12. We also have $K = x_0 + \text{span}\{u_1, \ldots, u_{n-r}\}$. Therefore, $K_H = \text{span}\{u_1, \ldots, u_{n-r}\}$.
- On the other hand, $\dim K_H = n - \text{rank}(A) = n - r$. Therefore, the set $\{u_1, \ldots, u_{n-r}\}$ is a basis for K_H. □

Starting in Definition 38, we have mentioned "the" RREF of a matrix, but do we know that a matrix can be row-reduced to only one RREF? Or might it be possible for a matrix to be row reducible to two different RREFs? This question is answered in the next theorem.

Theorem 3.18. *The RREF of a matrix is unique.*

Proof sketch. This is subtle; the claim is that if A is a matrix and B_1, B_2 are two RREF matrices such that A can be transformed to both B_1 and B_2 by elementary row operations, then $B_1 = B_2$. The key idea is from Question 4 from the practice problems for Week 8. Let $\text{rank}(A) = r$. Then B_1 and B_2 both have exactly r leading ones. Let's look first at B_1. Say that its leading ones occur in columns $i_1, i_2, \ldots, i_r$ where $1 \leq i_1 < i_2 < \cdots < i_r \leq n$. Consider the columns $Col_1(B_1), \ldots, Col_n(B_1)$ of B_1. Here are some things we can say:

1. $Col_{i_1}(B_1) = e_1 \in \mathbb{F}^m$, $Col_{i_2}(B_1) = e_2 \in \mathbb{F}^m$, etc., and $Col_{i_r}(B_1) = e_r \in \mathbb{F}^m$.
2. $Col_j(B_1) = 0 \in \mathbb{F}^m$ for all $1 \leq j < i_1$. (If $i_1 = 1$ then this isn't saying anything.)
3. For each $j = 1, \ldots, n$, the following are equivalent:

(a) $Col_j(B_1)$ **is** in the span of the columns to its left; i.e., $Col_j(B_1) \in \text{span}(Col_1(B_1), \ldots, Col_{j-1}(B_1))$.

(b) Column j does **not** contain a leading one; i.e., $j \notin \{i_1, i_2, \ldots, i_r\}$.

4. If $j \notin \{i_1, i_2, \ldots, i_r\}$ and column j is to the right of the first t leading ones and to the left of the last $r - t$ leading ones, then $Col_j(B_1) \in \text{span}(Col_{i_1}(B_1), Col_{i_2}(B_1), \ldots, Col_{i_t}(B_1))$. In fact, the assumption implies that all but the first t entries of column j must be 0; and if $Col_j(B_1) = (a_1, \ldots, a_t, 0, \ldots, 0)^T$ then

$$Col_j(B_1) = a_1 e_1 + \cdots + a_t e_t = a_1 Col_{i_1}(B_1) + \cdots + a_t Col_{i_t}(B_1).$$

Item 3 tells us how the linear dependencies of the columns of B_1 determine the columns which contain leading ones; and item 4 tells us how linear dependencies of the columns of B_1 completely determine the columns which do not contain leading ones.

Similar remarks apply to B_2; its entries are completely determined by the linear dependencies of its columns (in the same way). Now by assumption, B_1 can be transformed to B_2 by a sequence of elementary row operations. By Q4 from the practice problems for Week 8, the columns of B_1 and the columns of B_2 satisfy exactly the same linear dependencies. These remarks imply $B_1 = B_2$. □

Exercise: Let $A = [a_1\ a_2 \ldots\ a_n]$ be an $m \times n$ matrix and $B = [b_1\ b_2 \ldots\ b_n]$ be its RREF.

1. Prove that there exists an invertible matrix E such that $Ea_k = b_k$ for all $1 \leq k \leq n$.

2. Suppose $b_{i_1}, \ldots, b_{i_r}$ are the columns of B that contain the leading one. Prove that $\{a_{i_1}, \ldots, a_{i_r}\}$ is a basis for $\text{Col}(A)$.

3. Prove that $\text{Row}(B) = \text{Row}(A)$ and the nonzero rows of B form a basis for $\text{Row}(A)$.

4 Determinants

4.1 Definition of the determinant

To every square matrix $A \in \mathrm{M}_{n\times n}(\mathbb{F})$ there is an associated scalar $\det(A) \in \mathbb{F}$, called the **determinant** of A. In this chapter we will give a definition of $\det(A)$ and prove a number of properties of $\det(-)$ as a function $M_{n\times n}(\mathbb{F}) \to \mathbb{F}$. We'll start with the 2×2 and 3×3 cases.

2×2 **case**. Let $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \in M_{2\times 2}(\mathbb{F})$. Then

$$\det(A) = A_{11}A_{22} - A_{12}A_{21}.$$

3×3 **case**. Let $A = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \in M_{3\times 3}(\mathbb{F})$. Then

$$\det(A) = A_{11}A_{22}A_{33} + A_{12}A_{23}A_{31} + A_{13}A_{21}A_{32} - A_{11}A_{23}A_{32} - A_{12}A_{21}A_{33} - A_{13}A_{22}A_{31}.$$

There is a formula for the general $n \times n$ case; it is an alternating sum of $n!$ products where each product contains exactly one element from every row of A exactly one element from every column of A. More precisely, the formula for the determinant of an $n \times n$ matrix A is

$$\det(A) = \sum_{\sigma} \pm A_{1\sigma(1)}A_{2\sigma(2)} \cdots A_{n\sigma(n)}$$

where the sum is over all permutations σ of $\{1, 2, \ldots, n\}$, and the sign of the product corresponding to σ is determined by the "parity" of σ (which we will not define for now, but you can Google it if you are interested, or see the end of Section 4.5).

While this general formula has some theoretical interest, it is actually not useful for calculating determinants, nor is it helpful in proving the important theoretical properties of determinants. So we will not use the above definition. But we need *some* definition of determinants on which to build our theorems. The following recursive definition (which we will eventually see is equivalent to the formula above) is more amenable to our needs, and so we adopt it as our official definition of determinants. (In this section and the next, we are following the presentation in *Algebra*, by Michael Artin, Prentice Hall, 1991.)

Definition 39. *Let A be an $n \times n$ matrix with entries in the field $\mathbb{F}$. We define the determinant of A, denoted $\det(A)$ or $|A|$, as follows. Letting A_{ij} denote the entry of A in row i and column j:*

- *For $n = 1$, $\det(A) := A_{11}$. (Note that A_{11} is the single entry of A.)*
- *For $n \geq 2$, we define $\det(A)$ recursively as*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}),$$

where $\tilde{A}_{i1}$ denotes the $(n-1) \times (n-1)$ matrix obtained from A by deleting row i and column 1.

Example 47. 1. Suppose $n = 2$ and $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then $A_{11} = a$ and $A_{21} = c$, while $\tilde{A}_{11} = \begin{bmatrix} d \end{bmatrix}$ and $\tilde{A}_{21} = \begin{bmatrix} b \end{bmatrix}$. The $n = 1$ case of the definition gives $\det(\tilde{A}_{11}) = d$ and $\det(\tilde{A}_{21}) = b$. Thus the recursive definition gives

$$\det(A) = \sum_{i=1}^{2} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) = (-1)^2 a \cdot d + (-1)^3 c \cdot b = ad - bc.$$

2. Suppose $n = 3$ and $A = \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{bmatrix}$. Then $A_{11} = a_1$, $A_{21} = b_1$ and $A_{31} = c_1$, while

$$\tilde{A}_{11} = \begin{bmatrix} b_2 & b_3 \\ c_2 & c_3 \end{bmatrix}, \quad \tilde{A}_{21} = \begin{bmatrix} a_2 & a_3 \\ c_2 & c_3 \end{bmatrix}, \quad \text{and} \quad \tilde{A}_{31} = \begin{bmatrix} a_2 & a_3 \\ b_2 & b_3 \end{bmatrix}.$$

The recursive definition gives

$$\det(A) = \sum_{i=1}^{3} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) = a_1 \cdot \det\left(\begin{bmatrix} b_2 & b_3 \\ c_2 & c_3 \end{bmatrix}\right) - b_1 \cdot \det\left(\begin{bmatrix} a_2 & a_3 \\ c_2 & c_3 \end{bmatrix}\right) + c_1 \cdot \det\left(\begin{bmatrix} a_2 & a_3 \\ b_2 & b_3 \end{bmatrix}\right).$$

We still need to evaluate the three 2×2 determinants, which we can do using formula for the $n = 2$ case. In general, the definition of an $n \times n$ determinant requires calculating the determinants of n matrices of size $(n-1) \times (n-1)$; each of these latter determinants requires calculating the determinants of $n-1$ matrices of size $(n-2) \times (n-2)$; and so on.

3. In this example we illustrate the use of the notation $|A|$ for $\det(A)$.

$$\det \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{vmatrix} = 1 \begin{vmatrix} 5 & 6 \\ 8 & 10 \end{vmatrix} - 4 \begin{vmatrix} 2 & 3 \\ 8 & 10 \end{vmatrix} + 7 \begin{vmatrix} 2 & 3 \\ 5 & 6 \end{vmatrix} = (50-48) - 4(20-24) + 7(12-15) = -3.$$

Remarks.

- Our definition of determinants is also called cofactor expansion along the first column of A.
- More generally, if A is an $n \times n$ matrix with $n > 1$, then $\tilde{A}_{ij}$ denotes the $(n-1) \times (n-1)$ matrix obtained from A by deleting row i and column j.
- The scalar $(-1)^{i+j} \cdot \det(\tilde{A}_{ij})$ is called the cofactor of the entry of A in row i, column j.
- Hence the recursive definition of determinants expresses $\det(A)$ as the sum of the entries in the first column multiplied by their corresponding cofactors.
- One of the properties of determinants that we will prove later is that $\det(A)$ can be calculated by summing the entries of *any* fixed column multiplied by their corresponding cofactors; or by summing the entries of any fixed *row* multiplied by their corresponding cofactors. But until we have proved this, we will be careful not to use it.

Another important result we will prove is that a square matrix A is invertible if and only if $\det(A) \neq 0$. Let's prove this right now in the $n = 2$ case.

Theorem 4.1. *Let $A \in M_{2\times 2}(\mathbb{F})$. Then A is invertible if and only if $\det(A) \neq 0$. Moreover, if A is invertible, then*

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{bmatrix}.$$

Proof. ($\Leftarrow$) If $\det(A) \neq 0$, we can define a matrix

$$B = \frac{1}{\det(A)} \begin{bmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{bmatrix}.$$

We can verify easily that $AB = I$. Therefore A is invertible and $B = A^{-1}$.
($\Rightarrow$) Conversely, suppose A is invertible. So $\operatorname{rank}(A) = 2$. Therefore, the first column of A is nonzero. Hence $A_{11} \neq 0$ or $A_{21} \neq 0$.

- If $A_{11} \neq 0$, we apply an elementary row operation on A:

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \xrightarrow{R_2 - \frac{A_{21}}{A_{11}} R_1} \begin{bmatrix} A_{11} & A_{12} \\ 0 & A_{22} - \dfrac{A_{21}A_{12}}{A_{11}} \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} \\ 0 & \dfrac{\det(A)}{A_{11}} \end{bmatrix}.$$

  Since elementary operations do not change the rank, the matrix on the right also has rank 2. Therefore, its second row is non-zero. Hence $\dfrac{\det(A)}{A_{11}} \neq 0$. Thus $\det(A) \neq 0$.

- If $A_{21} \neq 0$, using a similar argument, we also have $\det(A) \neq 0$. □

4.2 Basic properties of determinants

Let's start proving some general properties of determinants.

Example 48. For all $n \geq 1$, $\det(I_n) = 1$.

Proof. When $n = 1$, the claim is true by the definition of determinants in the 1×1 case and the fact that 1 is the unique entry of I_1. Arguing by induction, assume that $n > 1$ and $\det(I_{n-1}) = 1$. Since

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

and recalling that our formula for $\det(I_n)$ is expansion by cofactors down the first column, we see that conveniently $(\tilde{I_n})_{11} = I_{n-1}$ and so

$$\det(I_n) \;=\; 1 \cdot \det(I_{n-1}) - 0 \cdot \det((\tilde{I_n})_{21}) + 0 \cdot \det((\tilde{I_n})_{31}) - \cdots + (-1)^{n+1} \cdot 0 \cdot \det((\tilde{I_n})_{n1}) \;=\; \det(I_{n-1})$$

so by induction, $\det(I_n) = 1$. □

More generally, we have the following.

Lemma 10. *If $A \in M_{n\times n}(\mathbb{F})$ is upper-triangular, then* $\det(A)$ *is equal to the product of its entries on the main diagonal. That is,*

$$\text{if} \qquad A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & 0 & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} \end{bmatrix} \qquad \text{then} \qquad \det(A) = \prod_{i=1}^{n} a_{ii}.$$

Proof sketch. By induction on n. When $n = 1$ the formula is clearly true. Assume $n > 1$ and the claim is true for $(n-1)\times(n-1)$ upper-triangular matrices. By definition,

$$\begin{aligned} \det(A) &= a_{11} \cdot \det(\tilde{A}_{11}) - 0 \cdot \det(\tilde{A}_{21}) + 0 \cdot \det(\tilde{A}_{31}) - \cdots \\ &= a_{11} \cdot \det(\tilde{A}_{11}). \end{aligned}$$

$\tilde{A}_{11}$ is upper-triangular of size $n-1 \times n-1$, so by induction, $\det(\tilde{A}_{11}) = a_{22}a_{33}\cdots a_{nn}$. □

Recall that we can transform any matrix A into a RREF matrix B using elementary row operations. If A is square, then B is automatically upper-triangular, so $\det(B)$ can be easily calculated using Lemma 10. Thus if we can quantify precisely how $\det(A)$ is related to $\det(B)$, we will be able to determine $\det(A)$ without having to use the recursive definition. That is our next goal. To get there, we will need to establish a sequence of lemmas.

Lemma 11. *If $A \in M_{n\times n}(\mathbb{F})$ and A has a row of zeros, then* $\det(A) = 0$.

Proof. By induction on n. If $n = 1$ then $A = \begin{bmatrix} 0 \end{bmatrix}$ and obviously $\det(A) = 0$. Assume $n > 1$ and the claim is true for matrices of smaller dimensions. Suppose $\text{Row}_{i_0}(A) = (0, 0, \ldots, 0)$. Consider the definition of $\det(A)$ by cofactor expansion along the first column. We claim that for each $i = 1, \ldots, n$, the product of a_{i1} with $(-1)^{i+1}\det(\tilde{A}_{i1})$ is equal to 0. Indeed, if $i \neq i_0$ then $\tilde{A}_{i1}$ has a row of zeros, so $\det(\tilde{A}_{i1}) = 0$ by induction. On the other hand, if $i = i_0$ then $a_{i_0 1} = 0$. Thus

$$\begin{aligned} \det(A) &= a_{11} \cdot \det(\tilde{A}_{11}) - a_{21} \cdot \det(\tilde{A}_{21}) + \cdots \pm a_{n1} \cdot \det(\tilde{A}_{n1}) \\ &= 0 - 0 + 0 - \cdots \\ &= 0. \end{aligned}$$

□

Lemma 12a. *If $A \in M_{n\times n}(\mathbb{F})$ and A has two equal adjacent rows, then* $\det(A) = 0$.

Note: "Adjacent" means "rows i and $i+1$" for some i.

Proof. Suppose $\text{Row}_{i_0}(A) = \text{Row}_{i_0+1}(A)$. Then for all $i \notin \{i_0, i_0{+}1\}$, $\tilde{A}_{i1}$ has two equal adjacent rows so $\det(\tilde{A}_{i1}) = 0$ by induction. Also, $\tilde{A}_{i_0,1} = \tilde{A}_{i_0+1,1}$ (this is subtle: draw a picture!) and $a_{i_0,1} = a_{i_0+1,1}$. Thus in the recursive definition of $\det(A)$, all terms are zero except for those at rows i_0 and $i_0{+}1$, and they cancel because they are equal and have opposite sign. □

Next, we explain a certain way in which det is a linear function. (It is *not* a linear transformation $M_{n\times n}(\mathbb{F}) \to \mathbb{F}$; exercise.)

Theorem 4.2. det *is "linear in each row." That is, if we fix* n, i_0, *and* $a_1, \ldots, a_{i_0-1}, a_{i_0+1}, \ldots, a_n \in \mathbb{F}^n$, *then for all* $b, c \in \mathbb{F}^n$ *and all* $\alpha \in \mathbb{F}$,

$$\det\begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & b+\alpha c & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix} = \det\begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & b & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix} + \alpha \cdot \det\begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & c & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix}$$

where $b + \alpha c$, b *and* c *were inserted in row* i_0.

Proof. We'll first explain the proof when $n = 4$ and $i_0 = 3$. Write

$$B = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ b_1 & b_2 & b_3 & b_4 \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \qquad C = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ c_1 & c_2 & c_3 & c_4 \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ b_1+\alpha c_1 & b_2+\alpha c_2 & b_3+\alpha c_3 & b_4+\alpha c_4 \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

Note that

$$\tilde{B}_{11} = \begin{bmatrix} a_{22} & a_{23} & a_{24} \\ b_2 & b_3 & b_4 \\ a_{42} & a_{43} & a_{44} \end{bmatrix} \qquad \tilde{C}_{11} = \begin{bmatrix} a_{22} & a_{23} & a_{24} \\ c_2 & c_3 & c_4 \\ a_{42} & a_{43} & a_{44} \end{bmatrix} \qquad \tilde{A}_{11} = \begin{bmatrix} a_{22} & a_{23} & a_{24} \\ b_2+\alpha c_2 & b_3+\alpha c_3 & b_4+\alpha c_4 \\ a_{42} & a_{43} & a_{44} \end{bmatrix}$$

By induction, $\det(\tilde{A}_{11}) = \det(\tilde{B}_{11}) + \alpha \cdot \det(\tilde{C}_{11})$. Similarly,

$$\begin{aligned} \det(\tilde{A}_{21}) &= \det(\tilde{B}_{21}) + \alpha \cdot \det(\tilde{C}_{21}) \quad \text{and} \\ \det(\tilde{A}_{41}) &= \det(\tilde{B}_{41}) + \alpha \cdot \det(\tilde{C}_{41}). \end{aligned}$$

Also note that $\tilde{B}_{31} = \tilde{C}_{31} = \tilde{A}_{31}$. Putting these facts together, we get

$$\begin{aligned} \det(A) &= a_{11} \cdot \det(\tilde{A}_{11}) - a_{21} \cdot \det(\tilde{A}_{21}) + (b_1 + \alpha c_1) \cdot \det(\tilde{A}_{31}) - a_{41} \cdot \det(\tilde{A}_{41}) \\ &= a_{11} \Big(\det(\tilde{B}_{11}) + \alpha \cdot \det(\tilde{C}_{11}) \Big) - a_{21} \Big(\det(\tilde{B}_{21}) + \alpha \cdot \det(\tilde{C}_{21}) \Big) \\ &\quad + (b_1 + \alpha c_1) \cdot \det(\tilde{A}_{31}) - a_{41} \Big(\det(\tilde{B}_{41}) + \alpha \cdot \det(\tilde{C}_{41}) \Big) \\ &= \Big(a_{11} \cdot \det(\tilde{B}_{11}) - a_{21} \cdot \det(\tilde{B}_{21}) + b_1 \cdot \det(\tilde{B}_{31}) - a_{41} \cdot \det(\tilde{B}_{41}) \Big) \\ &\quad + \alpha \Big(a_{11} \cdot \det(\tilde{C}_{11}) - a_{21} \cdot \det(\tilde{C}_{21}) + c_1 \cdot \det(\tilde{C}_{31}) - a_{41} \cdot \det(\tilde{C}_{41}) \Big) \\ &= \det(B) + \alpha \cdot \det(C). \end{aligned}$$

Next, we'll give the full proof, but warning: the idea of the proof is easier to grasp in the above special case than it is in the full proof.

The proof is by induction on n. The base case is left as an exercise. Assume $n \geq 2$ and denote

$$A = \begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & b + \alpha c & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix}, \quad B = \begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & b & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix}, \quad C = \begin{bmatrix} \text{—} & a_1 & \text{—} \\ & \vdots & \\ \text{—} & c & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{bmatrix}.$$

By definition,

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) = \left(\sum_{i \neq i_0} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) \right) + (-1)^{i_0+1} A_{i_0 1} \cdot \det(\tilde{A}_{i_0 1}).$$

Observe that

$$\tilde{A}_{i_0 1} = \tilde{B}_{i_0 1} = \tilde{C}_{i_0 1} \quad \text{and} \quad A_{i_0 1} = B_{i_0 1} + \alpha C_{i_0 1}.$$

For $i \neq i_0$, the matrices $\tilde{A}_{i1}, \tilde{B}_{i1}, \tilde{C}_{i1}$ have the same rows, except for one row k, where $k = i_0 - 1$ if $i < i_0$ and $k = i_0$ if $i > i_0$. Moreover, for this k (depending on i), the k-th rows of $\tilde{A}_{i1}$, $\tilde{B}_{i1}$, and $\tilde{C}_{i1}$ are $(b + \alpha c)$, b and c respectively. So by the induction hypothesis, we have

$$\det(\tilde{A}_{i1}) = \det(\tilde{B}_{i1}) + \alpha \det(\tilde{C}_{i1}), \quad \forall i \neq i_0.$$

We also have $A_{i1} = B_{i1} = C_{i1} \quad \forall i \neq i_0$. Plugging those equalities into the formula of $\det(A)$, we have

$$\begin{aligned}
\det(A) &= \sum_{i=1}^{n} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) \\
&= \sum_{i \neq i_0}^{n} (-1)^{i+1} A_{i1} \cdot \det(\tilde{A}_{i1}) + (-1)^{i_0+1} A_{i_0 1} \cdot \det(\tilde{A}_{i_0 1}) \\
&= \sum_{i \neq i_0} (-1)^{i+1} A_{i1} \cdot \big(\det(\tilde{B}_{i1}) + \alpha \det(\tilde{C}_{i1}) \big) + (-1)^{i_0+1} (B_{i_0 1} + \alpha C_{i_0 1}) \cdot \det(\tilde{A}_{i_0 1}) \\
&= \sum_{i \neq i_0} (-1)^{i+1} A_{i1} \cdot \det(\tilde{B}_{i1}) + \alpha \sum_{i \neq i_0} (-1)^{i+1} A_{i1} \cdot \det(\tilde{C}_{i1}) + (-1)^{i_0+1} B_{i_0 1} \cdot \det(\tilde{A}_{i_0 1}) + \alpha (-1)^{i_0+1} C_{i_0 1} \cdot \det(\tilde{A}_{i_0 1}) \\
&= \sum_{i \neq i_0} (-1)^{i+1} B_{i1} \cdot \det(\tilde{B}_{i1}) + \alpha \sum_{i \neq i_0} (-1)^{i+1} C_{i1} \cdot \det(\tilde{C}_{i1}) + (-1)^{i_0+1} B_{i_0 1} \cdot \det(\tilde{B}_{i_0 1}) + \alpha (-1)^{i_0+1} C_{i_0 1} \cdot \det(\tilde{C}_{i_0 1}) \\
&= \left(\sum_{i \neq i_0} (-1)^{i+1} B_{i1} \cdot \det(\tilde{B}_{i1}) + (-1)^{i_0+1} B_{i_0 1} \cdot \det(\tilde{B}_{i_0 1}) \right) + \alpha \left(\sum_{i \neq i_0} (-1)^{i+1} C_{i1} \cdot \det(\tilde{C}_{i1}) + (-1)^{i_0+1} C_{i_0 1} \cdot \det(\tilde{C}_{i_0 1}) \right) \\
&= \det(B) + \alpha \det(C).
\end{aligned}$$

□

To simplify notation, if $a_1, a_2, \ldots, a_n \in \mathbb{F}^n$ then we will use $\det(a_1, a_2, \ldots, a_n)$ to denote $\det(A)$ where A is the $n \times n$ matrix satisfying $\text{Row}_i(A) = a_i$ for $i = 1, \ldots, n$. (We should probably write $\text{Row}_i(A) = a_i^T$, but we won't, since the context makes clear that we are treating a_i as a row vector.) Then the previous theorem can be stated as follows: For all i_0 and all $a_1, \ldots, a_{i_0-1}, a_{i_0+1}, \ldots, a_n \in \mathbb{F}^n$, the function $x \mapsto \det(a_1, \ldots, a_{i_0-1}, x, a_{i_0+1}, \ldots, a_n)$ is a linear transformation from $\mathbb{F}^n$ to $\mathbb{F}$.

We can use the previous theorem to articulate the effect of type 2 elementary row operations on determinants.

Theorem 4.3 (Determinant after a type 2 elementary row operation)**.** *Let $A \in M_{n\times n}(\mathbb{F})$ and B be the matrix obtained from A by multiplying a row of A by a scalar c. Then* $\det(B) = c\det(A)$.

Proof. Suppose $A \xrightarrow{R_k \leftarrow cR_k} B$. Suppose $a_1, \ldots, a_n$ are the rows of A. Using Theorem 4.2, we have:

$$\begin{aligned}\det(B) &= \det(a_1, \ldots, ca_k, \ldots, a_n)\\ &= c\det(a_1, \ldots, a_k, \ldots, a_n)\\ &= c\det(A).\end{aligned}$$

□

We can also articulate the effect of a type 1 elementary row operation, *provided the two rows being swapped are adjacent.*

Theorem 4.4a (Determinant after type 1 elementary row operation – adjacent case)**.** *Let $A \in M_{n\times n}(\mathbb{F})$ and let B be a matrix obtained from A by swapping two adjacent rows. Then* $\det(B) = -\det(A)$.

Proof. Suppose $A \xrightarrow{R_i \leftrightarrow R_{i+1}} B$. Suppose $a_1, \ldots, a_{i-1}, b, c, a_{i+2}, \ldots, a_n$ are the rows of A; hence the rows of B are $a_1, \ldots, a_{i-1}, c, b, a_{i+2}, \ldots, a_n$. Let C be the $n \times n$ matrix whose rows are the rows of A, except for row i and row $i+1$, where the rows are both equal to $b + c$. Since C has two identical adjacent rows, by Lemma 12a, $\det(C) = 0$. On the other hand, using Theorem 4.2 first in row i and then in row $i+1$, we have

$$\begin{aligned}0 = \det(C) &= \det(a_1, \ldots, a_{i-1}, b{+}c, b{+}c, a_{i+2}, \ldots, a_n)\\ &= \det(a_1, \ldots, a_{i-1}, b, b{+}c, a_{i+2}, \ldots, a_n) + \det(a_1, \ldots, a_{i-1}, c, b{+}c, a_{i+2}, \ldots, a_n)\\ &= \det(a_1, \ldots, a_{i-1}, b, b, a_{i+2}, \ldots, a_n) + \det(a_1, \ldots, a_{i-1}, b, c, a_{i+2}, \ldots, a_n)\\ &\qquad + \det(a_1, \ldots, a_{i-1}, c, b, a_{i+2}, \ldots, a_n) + \det(a_1, \ldots, a_{i-1}, c, c, a_{i+2}, \ldots, a_n)\\ &= 0 + \det(A) + \det(B) + 0\end{aligned}$$

where the first and last determinants equal 0 by Lemma 12a. So $\det(B) = -\det(A)$. □

Now we can improve Lemma 12a by deleting the hypothesis of adjacent rows.

Lemma 12. *If a square matrix A has two identical rows, then* $\det(A) = 0$.

Proof. Suppose $a_1, \ldots, a_n$ are rows of A and $a_i = a_j$ for some $i < j$. Via some sequence of k successive swaps of *adjacent* rows, we can transform A to a matrix B in which the two equal rows are now adjacent. By Theorem 4.4a, each swap of adjacent rows in this transformation changes the determinant by a factor of -1. Thus we get

$$\det(A) = (-1)^k \det(B).$$

But $\det(B) = 0$ by Lemma 12a, which proves $\det(A) = 0$. □

And now we can improve Theorem 4.4a by deleting its hypothesis of adjacent rows.

Theorem 4.4 (Determinant after a type 1 elementary row operation)**.** *Let $A \in M_{n\times n}(\mathbb{F})$ and suppose $A \xrightarrow{R_i \leftrightarrow R_j} B$. Then* $\det(B) = -\det(A)$.

Proof. Suppose $a_1, \ldots, a_n$ are rows of A. Let C be an $n \times n$ matrix whose rows are the rows of A except for row i and row j, where those rows are both equal to $a_i + a_j$. Using the same argument as in the proof of Theorem 4.4a, but using Lemma 12 instead of Lemma 12a, we have the conclusion. □

Theorem 4.5 (Determinant after a type 3 elementary row operation)**.** *Let $A \in M_{n\times n}(\mathbb{F})$ and suppose $A \xrightarrow{R_i \leftarrow R_i + cR_j} B$. Then* $\det(B) = \det(A)$.

Proof. Suppose $a_1, \ldots, a_n$ are rows of A. We first prove for the case $i < j$. Using linearity of det in row i, we have

$$\begin{aligned}\det(B) &= \det(a_1, \ldots, \underbrace{a_i + ca_j}_{i}, \ldots, a_j, \ldots, a_n) \\ &= \det(a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n) + c\det(a_1, \ldots, a_j, \ldots, a_j, \ldots, a_n).\end{aligned}$$

The first determinant on the last line above is $\det(A)$. The second determinant on the last line is the determinant of a matrix having two equal rows. Hence the second determinant equals 0 by Lemma 12. Thus $\det(B) = \det(A)$ in the case $i < j$. Similarly, we have the same result for the case $j < i$. □

In summary, let A be a square matrix and B be a matrix obtained from A by an elementary row operation. Then

- For $A \xrightarrow{R_i \leftrightarrow R_j} B$, we have $\det(B) = -\det(A)$.
- For $A \xrightarrow{R_i \leftarrow cR_i} B$, we have $\det(B) = c\det(A)$.
- For $A \xrightarrow{R_i \leftarrow R_i + cR_j}$, we have $\det(B) = \det(A)$.

These facts give us an efficient way to calculate the determinant of a square matrix A: transform A to an upper-triangular matrix B using elementary row operations, keeping track of (i) the number of times, k, that a type 1 operation was used, and (ii) the constants $c_1, \ldots, c_\ell$ used in any type 2 operations. The determinant of B is easily calculated by Lemma 10. And $\det(B) = \det(A) \cdot (-1)^k c_1 c_2 \cdots c_\ell$ by the above facts.

Example 49. To find $\det \begin{bmatrix} 0 & 1 & 3 \\ -2 & -3 & -5 \\ 3 & -1 & 1 \end{bmatrix}$, do

$$\begin{aligned} A &= \begin{bmatrix} 0 & 1 & 3 \\ -2 & -3 & -5 \\ 3 & -1 & 1 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} -2 & -3 & -5 \\ 0 & 1 & 3 \\ 3 & -1 & 1 \end{bmatrix} \xrightarrow{R_3 \leftarrow R_3 + \frac{3}{2}R_1} \begin{bmatrix} -2 & -3 & -5 \\ 0 & 1 & 3 \\ 0 & -\frac{11}{2} & -\frac{13}{2} \end{bmatrix} \\ &\xrightarrow{R_3 \leftarrow 2R_3} \begin{bmatrix} -2 & -3 & -5 \\ 0 & 1 & 3 \\ 0 & -11 & -13 \end{bmatrix} \xrightarrow{R_3 \leftarrow R_3 + 11R_2} \begin{bmatrix} -2 & -3 & -5 \\ 0 & 1 & 3 \\ 0 & 0 & 20 \end{bmatrix} = B. \end{aligned}$$

B is upper-triangular, so $\det(B) = (-2) \cdot 1 \cdot 20 = -40$. We used one type 1 row operation ($R_1 \leftrightarrow R_2$) and one type 2 operation ($R_3 \leftarrow 2R_3$). So

$$\det(B) = \det(A) \cdot (-1) \cdot 2$$

and hence $\det(A) = 20$.

4.3 Determinants, invertibility, products, and transposes

Recall that in Theorems 4.3, 4.4 and 4.5 we have described the effect that an elementary row operation has on the determinant of a matrix. Since elementary matrices are the result of applying an elementary (row) matrix to the identity matrix I_n, and since $\det(I_n) = 1$, we can deduce the determinants of an elementary matrix.

Corollary 4.5.1. *Let E be an elementary matrix obtaining from I_n by an elementary row operation. Then*

1. *For a type 1 elementary row operation,* $\det(E) = -1$.
2. *For a type 2 elementary row operation with scalar $c \neq 0$,* $\det(E) = c$.
3. *For a type 3 elementary row operation,* $\det(E) = 1$.

In all cases, $\det(E) \neq 0$.

We can immediately deduce the following facts.

Corollary 4.5.2. *Let E be an elementary matrix obtaining from I_n by an elementary row operation. Then*

1. $\det(E^T) = \det(E)$.
2. $\det(E^{-1}) = \frac{1}{\det(E)}$.

Proof. It is enough to observe that E^T and E^{-1} are elementary matrices obtained from I_n by the same type of elementary operation that produced E; moreover, if the operation is type 2, say corresponding to $R_i \leftarrow aR_i$, then $E^T = E$ and E^{-1} is the elementary matrix corresponding to $R_i \leftarrow \frac{1}{c}R_i$. □

Theorem 4.6. *Let E be an $n \times n$ elementary matrix and $A \in M_{n\times n}(\mathbb{F})$. Then* $\det(EA) = \det(E)\det(A)$.

Proof. EA is the result of applying to A the row operation corresponding to E. Thus Theorems 4.3, 4.4 and 4.5 state that $\det(EA)$ is equal to $\det(A)$ multiplied by a factor determined by the row operation. Corollary 4.5.1 shows us that this factor is exactly $\det(E)$. □

Now we will exploit Corollary 4.5.2 and Theorem 4.6 plus our advanced knowledge of elementary row operations and elementary matrices to prove some deep properties of determinants. Our starting point is a routine strengthening of Theorem 4.6.

Corollary 4.6.1. *Let $A \in M_{n\times n}(\mathbb{F})$ and $E_1, \ldots, E_k$ be elementary matrices. Then*

1. $\det(E_1 \ldots E_k A) = \det(E_1) \cdots \det(E_k)\det(A)$.
2. $\det(E_1 \cdots E_k) = \det(E_1) \cdots \det(E_k)$.

Proof Sketch. Use Theorem 4.6 for Part 1. Part 2 is from Part 1 for $A = I_n$. □

Theorem 4.7 (Invertible Matrix Theorem (part 5))**.** *Let $A \in M_{n\times n}(\mathbb{F})$. Then A is invertible if and only if* $\det(A) \neq 0$.

Proof. ($\Rightarrow$) Suppose A is invertible, then $A = E_1 \dots E_q$, where $E_1, \dots, E_q$ are elementary matrices. Using Corollary 4.6.1(2) and the last claim in Corollary 4.5.1, we have

$$\det(A) = \det(E_1) \cdots \det(E_q) \neq 0.$$

($\Leftarrow$) Given $\det(A) \neq 0$. Suppose A is not invertible.
Let R be the RREF of A. Since A is not invertible, $\operatorname{rank}(A) < n$. Since $\operatorname{rank}(A)$ = the number of nonzero rows of R, we conclude that R has at least one zero row. Therefore, $\det(R) = 0$ by Lemma 11. On the other hand, since R is the RREF of A, we can transform R to A by a sequence of elementary row operations. Hence there exist elementary matrices $E_1, \dots, E_p$ such that

$$A = E_1 \cdots E_p R.$$

So by Corollary 4.6.1(1) we get $\det(A) = \det(E_1) \cdots \det(E_p) \det(R) = 0$, a contradiction. Therefore, the assumption is wrong and A is invertible. □

Corollary 4.7.1. *Let $A \in M_{n\times n}(\mathbb{F})$. If* $\operatorname{rank}(A) < n$, *then* $\det(A) = 0$.

Proof. If $\operatorname{rank}(A) < n$, A is not invertible. So $\det(A) = 0$. □

Theorem 4.8. *Let $A, B \in M_{n\times n}(\mathbb{F})$. Then* $\det(AB) = \det(A)\det(B)$.

Proof. Case 1: A is invertible. Then $A = E_1 \dots E_q$. Using Corollary 4.6.1, we have

$$\det(AB) = \det(E_1 \cdots E_q B) = \det(E_1) \cdots \det(E_q) \det(B) = \det(E_1 \cdots E_q) \det(B) = \det(A)\det(B).$$

Case 2: A is not invertible. Then AB is not invertible. By Theorem 4.7, $\det(A) = 0$ and $\det(AB) = 0$. So $\det(AB) = \det(A)\det(B)$. □

Theorem 4.9. *Let $A \in M_{n\times n}(\mathbb{F})$. Then* $\det(A) = \det(A^T)$.

Proof. Case 1: A is not invertible. Then $\operatorname{rank}(A) < n$. We have $\operatorname{rank}(A^T) = \operatorname{rank}(A)$ by Corollary 3.6.1, so $\operatorname{rank}(A^T) < n$. Then by Corollary 4.7.1., we have $\det(A) = \det(A^T) = 0$.
Case 2: A is invertible. Then there exist elementary matrices $E_1, \dots, E_k$ such that $A = E_1 \cdots E_k$. Then $A^T = (E_1 E_2 \cdots E_k)^T = E_k^T \cdots E_2^T E_1^T$ by Lemma 5 from Week 6, so

$$\begin{aligned}
\det(A^T) &= \det(E_k^T \cdots E_2^T E_1^T) \\
&= \det(E_k^T) \cdots \det(E_2^T) \det(E_1^T) && \text{by Corollary 4.6.1(2)} \\
&= \det(E_k) \cdots \det(E_2) \det(E_1) && \text{by Corollary 4.5.2(1)} \\
&= \det(E_1) \det(E_2) \cdots \det(E_k) && \text{because multiplication in } \mathbb{F} \text{ is commutative} \\
&= \det(E_1 E_2 \cdots E_k) && \text{Corollary 4.6.1(2) again} \\
&= \det(A).
\end{aligned}$$

□

4.4 Other Cofactor Expansions

We can use the fact that $\det(A) = \det(A^T)$ (Theorem 4.9) to convert all of our "row facts" about determinants to "column facts." In particular,

Corollary 4.9.1. *Suppose $A \in M_{n\times n}(\mathbb{F})$. If B is obtained from A by swapping two columns, then $\det(B) = -\det(A)$.*

Proof. If $A \xrightarrow{C_i \leftrightarrow C_j} B$, then $A^T \xrightarrow{R_i \leftrightarrow R_j} B^T$. Thus $\det(B^T) = -\det(A^T)$ by Theorem 4.4, so $\det(B) = \det(A)$ by Theorem 4.9. □

Theorem 4.10. *The determinant of A can be evaluated by cofactor expansion along any column. That is, for any fixed $j \in \{1, \ldots, n\}$, we have*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} A_{ij} \cdot \det(\tilde{A}_{ij}) = \sum_{i=1}^{n} A_{ij} \cdot \left(\underbrace{(-1)^{i+j} \det(\tilde{A}_{ij})}_{\text{cofactor of } A \text{ at } i,j} \right).$$

Note that second sum in the above theorem is the sum of the n entries of A in column j, each multiplied by the corresponding cofactor of A.

Before proving this theorem, let's see it illustrated in an example. Compare the following calculation to the one in Example 47(3), and observe that the alternating signs begin with $-$ when the column number is even.

Example 50. Using cofactor expansion in the second column, we get

$$\begin{aligned} \det \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix} &= -(2) \det \begin{bmatrix} 4 & 6 \\ 7 & 10 \end{bmatrix} + (5) \det \begin{bmatrix} 1 & 3 \\ 7 & 10 \end{bmatrix} - (8) \begin{bmatrix} 1 & 3 \\ 4 & 6 \end{bmatrix} \\ &= -2(40-42) + 5(10-21) - 8(6-12) \\ &= 4 - 55 + 48 \;=\; -3. \end{aligned}$$

Proof of Theorem 4.10. Let $a_1, \ldots, a_n$ be columns of A, so $A = [a_1 \ldots a_j \ldots a_n]$. Denote

$$B = [a_j \; a_1 \; a_2 \ldots a_{j-1} \; a_{j+1} \ldots a_n].$$

That is, B is obtained from A by cyclically shifting its first j columns to the right one position. Observe that $\tilde{A}_{ij} = \tilde{B}_{i1}$ and $A_{ij} = B_{i1}$ for each $i = 1, \ldots, n$. Also, observe that A can be obtained from B by $j-1$ successive swaps of adjacent columns (exercise), so $\det(A) = (-1)^{j-1} \det(B)$ by Corollary 4.9.1. We have

$$\det(B) = \sum_{i=1}^{n} (-1)^{i+1} B_{i1} \det(\tilde{B}_{i1}) = \sum_{i=1}^{n} (-1)^{i+1} A_{ij} \det(\tilde{A}_{ij}).$$

Hence

$$\det(A) = (-1)^{j-1} \det(B) = \sum_{i=1}^{n} (-1)^{i+j} A_{ij} \det(\tilde{A}_{ij}).$$

□

Corollary 4.10.1. *The determinant of A can be evaluated by cofactor expansion along any row. That is, for any fixed $i \in \{1, \ldots, n\}$, we have*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} A_{ij} \cdot \det(\tilde{A}_{ij}) = \sum_{j=1}^{n} A_{ij} \cdot \left(\underbrace{(-1)^{i+j} \det(\tilde{A}_{ij})}_{\text{cofactor of } A \text{ at } i,j} \right).$$

Proof sketch. Cofactor expansion of A along row i is the same as cofactor expansion of A^T along column i. Theorem 4.10 promises that the latter gives $\det(A^T)$, which equals $\det(A)$ by Theorem 4.9. □

Example 51. Using cofactor expansion along the third row,

$$\begin{aligned} \det \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{bmatrix} &= +(7) \det \begin{bmatrix} 2 & 3 \\ 5 & 6 \end{bmatrix} - (8) \det \begin{bmatrix} 1 & 3 \\ 4 & 6 \end{bmatrix} + (10) \begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix} \\ &= 7(12-15) - 8(6-12) + 10(5-8) \\ &= -21 + 48 - 30 \;=\; -3. \end{aligned}$$

When a row or column of a matrix contains lots of zeros, it often makes sense to calculate its determinant by first expanding by cofactors on that column or row.

Example 52. Find $\det(A)$ where

$$A = \begin{bmatrix} 2 & 3 & 1 & 5 \\ 1 & 0 & 0 & 0 \\ 8 & 0 & 6 & 2 \\ 1 & 0 & 0 & 7 \end{bmatrix}$$

Solution. It makes sense to expand by cofactors on the second column or the second row. Let's expand on the second row:

$$\det(A) = -(1) \det \begin{bmatrix} 3 & 1 & 5 \\ 0 & 6 & 2 \\ 0 & 0 & 7 \end{bmatrix} + (0) \det \begin{bmatrix} 2 & 1 & 5 \\ 8 & 6 & 2 \\ 1 & 0 & 7 \end{bmatrix} - (0) \det \begin{bmatrix} 2 & 3 & 5 \\ 8 & 0 & 2 \\ 1 & 0 & 7 \end{bmatrix} + (0) \det \begin{bmatrix} 2 & 3 & 1 \\ 8 & 0 & 6 \\ 1 & 0 & 0 \end{bmatrix}.$$

The first 3×3 matrix is upper triangular so its determinant is $3 \cdot 6 \cdot 7 = 126$. The determinants of the other 3×3 matrices do not need to be calculated because they are being multiplied by zeros. Hence $\det(A) = -126$.

4.5 A formula for A^{-1} and the Leibniz expansion of $\det(A)$

The results and proofs in this section are optional; you are not required to know them for this course. (But you might find them interesting anyway!) Let's start with an easy result.

Lemma 13. *Suppose $A \in M_{n\times n}(\mathbb{F})$ and let its columns be $a_1, \ldots, a_n$. Fix $i, j \in \{1, \ldots, n\}$ and let B be the matrix obtained from A by replacing column i with e_j. That is, $A = [a_1 \cdots a_{i-1}\ a_i\ a_{i+1} \cdots a_n]$ and $B = [a_1 \cdots a_{i-1}\ e_j\ a_{i+1} \cdots a_n]$. Then $\det(B) = (-1)^{i+j} \det(\tilde{A}_{ji})$.*

Proof. Consider the expansion of $\det(B)$ by cofactors along column i. Because the i-th column of B is e_j, all products in the cofactor expansion will be 0 except for the product corresponding to row j, where e_j is 1. Thus

$$\begin{aligned}\det(B) &= (-1)^{1+i}(0)\det(\tilde{B}_{1i}) + \cdots + (-1)^{j+i}(1)\det(\tilde{B}_{ji}) + \cdots + (-1)^{n+i}(0)\det(\tilde{B}_{ni}) \\ &= (-1)^{j+i}(1)\det(\tilde{B}_{ji}) \\ &= (-1)^{i+j}\det(\tilde{A}_{ji}) \qquad \text{since } \det(\tilde{B}_{ji}) = \det(\tilde{A}_{ji}) \text{ (exercise).}\end{aligned}$$

□

We also need the following technical result.

Lemma 14. *Suppose $C \in M_{n\times n}$, and let its entry at row i, column j be C_{ij}. Fix $i, j \in \{1, \ldots, n\}$ and let X_{ij} be the $n \times n$ matrix obtained from I_n by replacing column i with $\mathrm{Col}_j(C)$. That is,*

$$X_{ij} = [e_1\ e_2 \cdots e_{i-1}\ \mathrm{Col}_j(C)\ e_{i+1} \cdots e_n].$$

Then $\det(X_{ij}) = C_{ij}$.

Proof. Using type 3 elementary column operations, we can transform X_{ij} as follows:

$$X_{ij} = \begin{bmatrix} 1 & 0 & \cdots & 0 & C_{1j} & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & C_{2j} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & C_{(i-1)j} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & C_{ij} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & C_{(i+1)j} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & C_{(n-1)j} & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & C_{nj} & 0 & \cdots & 0 & 1 \end{bmatrix} \xrightarrow{\text{type 3 column ops}} \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & C_{ij} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

Type 3 elementary column operations do not change the determinant (exercise). The right-hand matrix is upper-triangular, so its determinant is the product of its diagonal entries, which is C_{ij}. □

Now we can prove the following formula for the inverse of a matrix.

Theorem 4.11. *Suppose $A \in M_{n\times n}(\mathbb{F})$ and A is invertible. Then $A^{-1} = \frac{1}{\det(A)}Q$ where Q is the $n \times n$ matrix whose row i, column j entry Q_{ij} is the row j, column i cofactor of A (for all i and j). That is,*

$$Q_{ij} = (-1)^{i+j}\det(\tilde{A}_{ji}).$$

Proof. Let $C = A^{-1}$. Fix $i, j \in \{1, \ldots, n\}$. Let X_{ij} be the matrix obtained from I_n by replacing column i with $\mathrm{Col}_j(C)$. Then $\det(X_{ij}) = C_{ij}$ by Lemma 14. Now let the columns of A be $a_1, \ldots, a_n$ so $A = [a_1\ a_2 \cdots a_n]$. Note also that $X_{ij} = [e_1 \cdots e_{i-1}\ \mathrm{Col}_j(C)\ e_{i+1} \cdots e_n]$. Hence

$$\begin{aligned}AX_{ij} &= [Ae_1\ Ae_2 \cdots Ae_{i-1}\ A\mathrm{Col}_j(C)\ Ae_{i+1} \cdots Ae_n] \\ &= [\ a_1\ \ a_2\ \ \cdots\ a_{i-1}\ \ A\mathrm{Col}_j(C)\ \ a_{i+1}\ \cdots\ a_n]\ .\end{aligned}$$

Also note that $A\text{Col}_j(C) = e_j$ because $C = A^{-1}$. Hence AX_{ij} equals the matrix B obtained from A by replacing column i with e_j. It follows from Lemma 13 that $\det(AX_{ij}) = (-1)^{i+j}\det(\tilde{A}_{ji})$. But also $\det(AX_{ij}) = \det(A)\det(X_{ij}) = \det(A)\cdot C_{ij}$. These facts prove $C_{ij} = \frac{1}{\det(A)}(-1)^{i+j}\det(\tilde{A}_{ji})$. Thus if we define Q as in the statement of the theorem, then we have $C = \frac{1}{\det(A)}Q$. □

As a quick reality check, let's work out what the last theorem is saying when $n = 2$. If

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

then the matrix Q is

$$Q = \begin{bmatrix} (-1)^{1+1}\det(\tilde{A}_{11}) & (-1)^{1+2}\det(\tilde{A}_{21}) \\ (-1)^{2+1}\det(\tilde{A}_{12}) & (-1)^{2+2}\det(\tilde{A}_{22}) \end{bmatrix} = \begin{bmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{bmatrix}$$

Hence if A is invertible, then Theorem 4.11 tells us that

$$A^{-1} = \frac{1}{\det(A)}\begin{bmatrix} A_{22} & -A_{12} \\ -A_{21} & A_{11} \end{bmatrix}$$

which agrees with our formula in Theorem 4.1.

The formula for A^{-1} given in Theorem 4.11 has little practical value. As n grows, the time needed to carry out the calculation of all the determinants defining the entries of Q becomes prohibitive. A much better way to calculate inverses is the method given in Section 3.4. However, the formula has some interesting consequences. Here is one.

Corollary 4.11.1. *Suppose $A \in M_{n\times n}(\mathbb{Q})$ and suppose that every entry of A is an integer. If $|\det(A)| = 1$, then (A is invertible and) every entry of A^{-1} is also an integer.*

Proof. A is invertible because $\det(A) \neq 0$. Consider the matrix Q in the formula for A^{-1} in Theorem 4.11. Its entries are cofactors of A, which are $\pm$ determinants of $(n-1)\times(n-1)$ submatrices of A. One can easily prove by induction that a determinant of a matrix with integer entries is always an integer. Thus Q has integer entries. Then

$$A^{-1} = \frac{1}{\det(A)}Q = \pm Q$$

so A^{-1} also has integer entries. □

We will close this section by deducing an explicit formula for $\det(A)$, sometimes called the *Leibniz expansion*. Suppose A is $n \times n$, let its entries be denotes A_{ij}, and let its rows be denoted $a_1, \ldots, a_n$. We can use the entries in each row to describe the row as a linear combination of $e_1, \ldots, e_n$. Namely,

$$a_i = A_{i1}e_1 + A_{i2}e_2 + \cdots + A_{in}e_n \quad \text{for } i = 1, \ldots, n.$$

Using this formula for a_1 and applying linearity of det in the first row, we get

$$\det(A) = A_{11}\det\begin{pmatrix} \text{—} & e_1 & \text{—} \\ \text{—} & a_2 & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{pmatrix} + A_{12}\det\begin{pmatrix} \text{—} & e_2 & \text{—} \\ \text{—} & a_2 & \text{—} \\ & \vdots & \\ \text{—} & a_n & \text{—} \end{pmatrix} + \cdots + A_{1n}\det\begin{pmatrix} \text{—} & e_n & \text{—} \\ \text{—} & a_2 & \text{—} \\ & \vdots & \\ \text{—} & r_n & \text{—} \end{pmatrix}.$$

Repeating in the second row of each of these matrices, using linearity of det in the second row, we get an expression for $\det(A)$ involving n^2 terms. Eventually, we get an expression for $\det(A)$ involving n^n terms, looking like

$$\det(A) = \sum_{i_1,i_2,\ldots,i_n=1}^{n} A_{1i_1}A_{2i_2}\cdots A_{ni_n} \det \begin{pmatrix} \text{—} & e_{i_1} & \text{—} \\ \text{—} & e_{i_2} & \text{—} \\ & \vdots & \\ \text{—} & e_{i_n} & \text{—} \end{pmatrix}$$

The sum is over all possible choices of $i_1, \ldots, i_n \in \{1, \ldots, n\}$. Many terms in this enormous sum will equal 0; if $(i_1, i_2, \ldots, i_n)$ is not a permutation of $\{1, \ldots, n\}$, then the matrix with rows $e_{i_1}, \ldots, e_{i_n}$ has two equal rows, so its determinant is 0. Thus the sum simplifies to

$$\det(A) \quad = \quad \sum_{\sigma \in S_n} A_{1\sigma(1)}A_{2\sigma(2)}\cdots A_{n\sigma(n)} \det \begin{pmatrix} \text{—} & e_{\sigma(1)} & \text{—} \\ \text{—} & e_{\sigma(2)} & \text{—} \\ & \vdots & \\ \text{—} & e_{\sigma(n)} & \text{—} \end{pmatrix}$$

where the sum is now over all permutations σ of $\{1, \ldots, n\}$. Note that for each permutation σ, the matrix

$$P_\sigma := \begin{bmatrix} \text{—} & e_{\sigma(1)} & \text{—} \\ \text{—} & e_{\sigma(2)} & \text{—} \\ & \vdots & \\ \text{—} & e_{\sigma(n)} & \text{—} \end{bmatrix}$$

is obtained by permuting the rows of I_n. Hence its determinant is $+1$ or -1 depending on whether P_σ can be constructed from I_n using an even number of row swaps or an odd number of row swaps. Define the *parity* of σ to be **even** if $\det(P_\sigma) = 1$, and define it to be **odd** if $\det(P_\sigma) = -1$. We have proved:

Theorem 4.12. *If $A \in M_{n\times n}(\mathbb{F})$ then*

$$\det(A) = \sum_{\sigma} \operatorname{sgn}(\sigma) A_{1\sigma(1)}A_{2\sigma(2)}\cdots A_{n\sigma(n)}$$

where the sum is over all permutations σ of $\{1, \ldots, n\}$, and where $\operatorname{sgn}(\sigma) = +1$ if the parity of σ is even, and $\operatorname{sgn}(\sigma) = -1$ if the parity of σ is odd.

Like the formula for A^{-1} in Theorem 4.11, this formula for $\det(A)$ is of almost no practical value. However, it has some useful theoretical consequences. For example, it makes obvious the earlier claim that if the entries of a matrix are all integers, then $\det(A)$ is also an integer. We can "see" this since $\det(A)$ is an alternating sum of products of the entries of A.

4.6 Summary–Important Facts About Determinants

.

Let $A \in M_{n\times n}(\mathbb{F})$. Then

- $n = 1 : \det(A) = A_{11}$.
- $n = 2 : \det(A) = A_{11}A_{22} - A_{12}A_{21}$.
- $n \geq 2$: Cofactor expansion along column j:

$$\det(A) = \sum_{i=1}^{n}(-1)^{i+j}A_{ij} \cdot \det(\tilde{A}_{ij}).$$

  Cofactor expansion along row i:

$$\det(A) = \sum_{j=1}^{n}(-1)^{i+j}A_{ij} \cdot \det(\tilde{A}_{ij}).$$

- If B is obtained from A by interchanging two rows or two columns of A, $\det(B) = -\det(A)$.
- If B is obtained from A by multiplying a row or a column of A by a scalar c, $\det(B) = c\det(A)$.
- If B is obtained from A by adding a multiple of row (column) i to row (column) j, for $i \neq j$, then $\det(B) = \det(A)$.
- If A has two equal rows (columns), then $\det(A) = 0$.
- If A has a zero row (column), then $\det(A) = 0$.
- $\det(A) = \det(A^T)$.
- The determinant of an upper triangular matrix is the product of its diagonal entries. In particular, $\det(I_n) = 1$.
- A is invertible if and only if $\det(A) \neq 0$. If A is invertible, $\det(A^{-1}) = \dfrac{1}{\det(A)}$.
- If $B \in M_{n\times n}(\mathbb{F})$, then $\det(AB) = \det(A)\det(B)$.

5 Diagonalization

5.1 Eigenvalues and Eigenvectors

Motivation:

- Given $A \in M_{n\times n}(\mathbb{F})$. For almost all vector $x \in \mathbb{F}^n$, Ax is not in the same direction as x, that is $Ax \neq \lambda x$ for any $\lambda \in \mathbb{F}$. However, there exist special nonzero vectors v that are in the same direction as Av, which we call eigenvectors. The (unique) corresponding scalar $\lambda \in \mathbb{F}$ such that $Av = \lambda v$ is called the eigenvalue of A corresponding to v.

- Why are eigenvectors special? Here are some reasons:

  - If v is an eigenvector of a matrix $A \in M_{n\times n}(\mathbb{F})$ with $Av = \lambda v$, for some $\lambda \in \mathbb{F}$, then

$$A^2v = A(Av) = A(\lambda v) = \lambda Av = \lambda^2 v,$$

$$A^3v = A(A^2v) = A(\lambda^2 v) = \lambda^2 Av = \lambda^3 v.$$

    Indeed, we can prove by induction that $A^m v = \lambda^m v$ for $m = 1, 2, \ldots$. That is, v is also an eigenvector of A^m for any positive integer m.

  - In many applications, we would like to know A^m for $m = 1, 2, \ldots$. For example, consider $A = \begin{bmatrix} 0.9 & 0.3 \\ 0.1 & 0.7 \end{bmatrix}$. Here are some first powers of A:

$$A^2 = \begin{bmatrix} 0.84 & 0.48 \\ 0.16 & 0.52 \end{bmatrix}, \; A^3 = \begin{bmatrix} 0.804 & 0.588 \\ 0.196 & 0.412 \end{bmatrix}, \; A^4 = \begin{bmatrix} 0.7824 & 0.6528 \\ 0.2176 & 0.3472 \end{bmatrix}, \ldots,$$

$$A^{2021} = \begin{bmatrix} 0.875 & 0.875 \\ 0.125 & 0.125 \end{bmatrix} + \text{a matrix whose entries are almost zero.}$$

    Indeed, A^{2021} was found by using the eigenvalues and eigenvectors of A, not by multiplying 2021 matrices (see the spectral theorem later on).

Definition 40. *Let A be a square matrix in $M_{n\times n}(\mathbb{F})$.*

- *A nonzero vector $v \in \mathbb{F}^n$ is called an eigenvector of A if there exists a scalar $\lambda \in \mathbb{F}$ such that $Av = \lambda v$. Such λ is called the eigenvalue of A corresponding to the eigenvector v and (λ, v) is called an eigenpair of the matrix A.*

- *If $\lambda \in \mathbb{F}$ is an eigenvalue of A, the set*

$$\begin{aligned} E_\lambda &= \{\text{eigenvectors of } A \text{ corresponding to } \lambda\} \cup \{0\} \\ &= \{v \in \mathbb{F}^n : Av = \lambda v\} \\ &= \{v \in \mathbb{F}^n : (A - \lambda I_n)v = 0\} = N(A - \lambda I_n) \end{aligned}$$

  is called the eigenspace of A corresponding to λ.

Remark 22. Let $A \in M_{n\times n}(\mathbb{F})$ and $\lambda \in \mathbb{F}$ be an eigenvalue of A. From the above definitions,

1. A vector $v \in \mathbb{F}^n$ is an eigenvector of A corresponding to the eigenvalue λ iff v is a non-zero solution of the linear system $(A - \lambda I_n)v = 0$.

2. Since $E_\lambda = N(A - \lambda I_n)$, E_λ is a subspace of $\mathbb{F}^n$. So $\dim(E_\lambda) \leq n$. Also, since E_λ contains at least one eigenvector, $E_\lambda \neq \{0\}$. Hence, $\dim(E_\lambda) \geq 1$.

Remark 23. Let $C \in M_{m\times n}(\mathbb{F})$. To solve a homogeneous system $Cx = 0$, $x \in \mathbb{F}^n$, we use elementary row operations to transform the augmented matrix $(C \mid 0)$ into its RREF $(C' \mid b')$. Since the right-hand side of the homogeneous system $Cx = 0$ is a zero vector, applying elementary row operations to the augmented matrix $(C \mid 0)$ does not change its last column, which is always the zero vector. Therefore, when solving a homogeneous system, it is standard practice to apply elementary row operations to the coefficient matrix C to transform C into RREF C'. Then we write the homogeneous system corresponding to the RREF and find the general solution of $Cx = 0$.

The next theorem tells us how to find all eigenvalues of a given square matrix.

Theorem 5.1. *Let $A \in M_{n\times n}(\mathbb{F})$. Then a scalar λ is an eigenvalue of A if and only if* $\det(A-\lambda I_n) = 0$.

Proof.

$$\begin{aligned}
\lambda \text{ is an eigenvalue of } A &\Leftrightarrow \exists v \in \mathbb{F}^n, v \neq 0 \text{ such that } Av = \lambda v.\\
&\Leftrightarrow \exists v \in \mathbb{F}^n, v \neq 0 \text{ such that } (A - \lambda I_n)v = 0.\\
&\Leftrightarrow (A - \lambda I_n)x = 0 \text{ has more than one solution } x \in \mathbb{F}^n.\\
&\Leftrightarrow (A - \lambda I_n) \text{ is not invertible.}\\
&\Leftrightarrow \det(A - \lambda I_n) = 0.
\end{aligned}$$

□

Example 53. Find all eigenvalues of $A = \begin{bmatrix} -1 & 6 & 3 \\ 1 & 0 & -1 \\ -3 & 6 & 5 \end{bmatrix} \in M_{3\times 3}(\mathbb{R})$. Find a basis for each eigenspace of A.

Proof. We have

$$\begin{aligned}
\det(A - tI) &= \begin{vmatrix} -1-t & 6 & 3 \\ 1 & -t & -1 \\ -3 & 6 & 5-t \end{vmatrix} = (-1-t)\begin{vmatrix} -t & -1 \\ 6 & 5-t \end{vmatrix} + (-1)6\begin{vmatrix} 1 & -1 \\ -3 & 5-t \end{vmatrix} + 3\begin{vmatrix} 1 & -t \\ -3 & 6 \end{vmatrix}\\
&= -(t+1)[t(t-5)+6] - 6(5-t-3) + 3(6-3t)\\
&= -(t+1)(t^2-5t+6) - 6(2-t) + 9(2-t)\\
&= -(t+1)(t-3)(t-2) + 3(2-t)\\
&= -(t-2)[(t+1)(t-3)+3] = -(t-2)(t^2-2t) = -t(t-2)^2.
\end{aligned}$$

So the eigenvalues of A are $\lambda_1 = 0$ and $\lambda_2 = 2$.

For $\lambda_1 = 0$: We solve $(A-\lambda_1 I_3)v = 0$ to find the corresponding eigenvectors. Applying elementary row operations to the coefficient matrix $(A - \lambda_1 I_3)$ yields

$$A-\lambda_1 I_3 = \begin{bmatrix} -1 & 6 & 3 \\ 1 & 0 & -1 \\ -3 & 6 & 5 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} 1 & 0 & -1 \\ -1 & 6 & 3 \\ -3 & 6 & 5 \end{bmatrix} \begin{matrix} \xrightarrow{R_2+R_1} \\ \xrightarrow{R_3+3R_1} \end{matrix} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 6 & 2 \\ 0 & 6 & 2 \end{bmatrix} \xrightarrow{R_3-R_2} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 6 & 2 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{\frac{1}{6}R_2} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & \frac{1}{3} \\ 0 & 0 & 0 \end{bmatrix}.$$

The corresponding system of equation is

$$\begin{aligned} x_1 \qquad & -x_3 = 0 \\ x_2 \quad & +\frac{1}{3}x_3 = 0 \end{aligned}$$

The free variable is x_3. Let $x_3 = 3s$. Then $x_1 = x_3 = 3s$ and $x_2 = -\frac{1}{3}x_3 = -s$. Therefore

$$E_{\lambda_1} = \left\{ \begin{bmatrix} 3s \\ -s \\ 3s \end{bmatrix} : s \in \mathbb{F} \right\} = \left\{ s \begin{bmatrix} 3 \\ -1 \\ 3 \end{bmatrix} : s \in \mathbb{F} \right\}.$$

A basis for E_{λ_1} is $\left\{ \begin{bmatrix} 3 \\ -1 \\ 3 \end{bmatrix} \right\}$.

For $\lambda_2 = 2$: We solve $(A-\lambda_2 I_3)v = 0$ to find the corresponding eigenvectors. Applying elementary row operations to the coefficient matrix $(A - \lambda_2 I_3)$ yields

$$A - \lambda_2 I_3 = \begin{bmatrix} -3 & 6 & 3 \\ 1 & -2 & -1 \\ -3 & 6 & 3 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} 1 & -2 & -1 \\ -3 & 6 & 3 \\ -3 & 6 & 3 \end{bmatrix} \begin{matrix} \xrightarrow{R_2+3R_1} \\ \xrightarrow{R_2+3R_1} \end{matrix} \begin{bmatrix} 1 & -2 & -1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The free variables are x_2 and x_3. Let $x_2 = s$ and $x_3 = t$. Then $x_1 = 2s + t$ and

$$E_{\lambda_2} = \left\{ \begin{bmatrix} 2s+t \\ s \\ t \end{bmatrix} : s, t \in \mathbb{F} \right\} = \left\{ s \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} : s, t \in \mathbb{F} \right\}.$$

A basis for E_{λ_2} is $\left\{ \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$. □

Definition 41. *Let $A \in M_{n\times n}(\mathbb{F})$. The polynomial of variable t, $p_A(t) := \det(A - tI_n)$, is called the characteristic polynomial of A. That is,*

$$p_A(t) = \det(A - tI_n) = \begin{vmatrix} a_{11} - t & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - t & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - t \end{vmatrix}.$$

Theorem 5.2 (Properties of Characteristic Polynomials)**.** *Let $A \in M_{n\times n}(\mathbb{F})$. Denote* $\operatorname{tr}(A) = \sum_{i=1}^{n} a_{ii}$.

1. *Then*
$$p_A(t) = (-1)^n t^n + (-1)^{n-1}\operatorname{tr}(A)t^{n-1} + c_{n-2}t^{n-2} + \cdots + c_1 t + \det(A).$$
That is, $p_A(t)$ is a polynomial of degree n with leading coefficient $(-1)^n$ and constant coefficient $\det(A)$. Also, the coefficient of t^{n-1} in $p_A(t)$ is $(-1)^{n-1}\operatorname{tr}(A)$. In addition, the matrix A has at most n distinct eigenvalues.

2. *If $B \in M_{n\times n}(\mathbb{F})$ is similar to A, then $p_B(t) = p_A(t)$. (Recall: Let $A, B \in M_{n\times n}(\mathbb{F})$. The matrix B is said to be similar to A if there exists an invertible matrix P such that $B = P^{-1}AP$.)*

Proof Sketch. 1. The determinant $\det(A - tI_n)$ can be computed by cofactor expansion along the first column
$$p_A(t) = (a_{11} - t)(a_{22} - t)\dots(a_{nn} - t) + (\text{terms of degree} \le n - 2).$$
Or, we can use Theorem 4.12 to compute $\det(A - tI_n)$. That is, each entry of $(A - tI_n)$ is a polynomial in $\mathbb{F}[t]$ of degree ≤ 1. Hence each product of n entries is a polynomial in $\mathbb{F}[t]$ of degree $\le n$. Since $p_A(t)$ is an alternating sum of such entries, $\deg(p_A(t)) \le n$.

On the other hand, the only contributions of t to $p_A(t)$ come from the diagonal entries of $(A - tI_n)$. A product in the complete expansion either has all diagonal entries, or at most $(n - 2)$ of them. Therefore,
$$p_A(t) = (a_{11} - t)(a_{22} - t)\dots(a_{nn} - t) + (\text{terms of degree} \le n - 2).$$
The coefficients of t^n and t^{n-1} in $p_A(t)$ come entirely from
$$(a_{11} - t)(a_{22} - t)\dots(a_{nn} - t).$$
Therefore, $p_A(t)$ is a polynomial of degree n with leading coefficient $(-1)^n$ and the coefficient of t^{n-1} in $p_A(t)$ is $(-1)^{n-1}\sum_{i=1}^{n} a_{ii} = (-1)^{n-1}\operatorname{tr}(A)$. Hence, we can write
$$p_A(t) = \det(A - tI_n) = (-1)^n t^n + (-1)^{n-1}\operatorname{tr}(A)t^{n-1} + c_{n-2}t^{n-2} + \cdots + c_1 t + c_0 \in \mathrm{P}_n(\mathbb{F}),$$
Let $t = 0$, we have
$$p_A(0) = \det(A - 0\ I_n) = (-1)^n 0^n + (-1)^{n-1}\operatorname{tr}(A)0^{n-1} + \cdots + c_1 0 + c_0$$
$$\det(A) = c_0.$$
Also, since a polynomial of degree n has at most n roots, A has at most n distinct eigenvalues.

2. We have
$$\begin{aligned} p_B(t) &= \det(B - tI_n) = \det(P^{-1}(A - tI_n)P) = \det(P^{-1})\det(A - tI_n)\det(P) \\ &= p_A(t)\det(P^{-1})\det(P) = p_A(t)\det(P^{-1}P) = p_A(t). \end{aligned}$$

□

Next we will revisit the connection between matrices and linear operators from the perspective of eigenvalues and eigenvectors.

Remark 24. Let $A \in M_{n\times n}(\mathbb{F})$. Recall that $L_A(x) = Ax, \forall x \in \mathbb{F}^n$ and $A = [L_A]_\beta$, where β is the standard ordered basis for $\mathbb{F}^n$.

1. Suppose $\lambda \in \mathbb{F}$ is an eigenvalue of A. A vector $v \in \mathbb{F}^n$ is an eigenvector of A corresponding to the eigenvalue $\lambda \Leftrightarrow L_A(v) = \lambda v$ and $v \neq 0 \Leftrightarrow (L_A - \lambda \operatorname{Id}_{\mathbb{F}^n})(v) = 0$ and $v \neq 0 \Leftrightarrow v \in N(L_A - \lambda \operatorname{Id}_{\mathbb{F}^n})$ and $v \neq 0$.

2. A scalar $\lambda \in \mathbb{F}$ is an eigenvalue of $A \Leftrightarrow (A - \lambda I_n)$ is not invertible $\Leftrightarrow L_{(A-\lambda I_n)}$ is not invertible $\Leftrightarrow (L_A - \lambda \operatorname{Id}_{\mathbb{F}^n})$ is not invertible (Since $L_{A-\lambda I_n} = L_A - \lambda \operatorname{Id}_{\mathbb{F}^n}$).

For the remainder of the course, linear transformations from a vector space V to itself are called linear operators. Let's define eigenvalues and eigenvectors for linear operators.

Definition 42.
- *Let $T : V \to V$ be a linear mapping on a vector space V. A scalar $\lambda \in \mathbb{F}$ is called an eigenvalue of the linear operator T if there exists a nonzero vector $v \in V$ such that $T(v) = \lambda v$. Such vector v is called an eigenvector of T corresponding to the eigenvalue λ and (λ, v) is called an eigenpair of the linear mapping T.*
- *Let $T : V \to V$ be a linear operator on an n-dimensional vector space V with ordered basis β. We define the characteristic polynomial of T to be the characteristic polynomial of $A = [T]_\beta$.*

Example 54.
1. Let $C^\infty(\mathbb{R})$ be the set of all functions $f : \mathbb{R} \to \mathbb{R}$ having derivatives of all orders. We can verify that $C^\infty(\mathbb{R})$ is a vector space over $\mathbb{R}$. Consider

$$T : C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R}), \quad T(f(x)) = f'(x).$$

We can verify that T is a linear mapping. If $(\lambda, p(x))$ is an eigenpair of T then

$$T(p(x)) = \lambda p(x) \Rightarrow p'(x) = \lambda p(x) \Rightarrow p(x) = ce^{\lambda x}, \text{ where } c \in \mathbb{R}, c \neq 0.$$

2. Consider $T : \mathbb{R}^2 \to \mathbb{R}^2$ be the linear operator that rotates each vector in the plane through an angle of 90 degree counterclockwise. Then T has no eigenvectors and no eigenvalues.

Theorem 5.3. *Let $T : V \to V$ be a linear operator on a vector space V. Then*

1. *A scalar $\lambda \in \mathbb{F}$ is an eigenvalue of T if and only if $(T - \lambda \operatorname{Id}_V)$ is not invertible.*
2. *Let λ be an eigenvalue of T. A vector $v \in V$ is an eigenvector of T corresponding to λ if and only if $v \neq 0$ and $v \in N(T - \lambda \operatorname{Id}_V)$.*

Proof. Exercise. □

Remark 25. The characteristic polynomial of a linear mapping $T : V \to V$ is defined via the characteristic polynomial of a matrix representation of T in an ordered basis of V. The following lemma will prove that the characteristic polynomial of a linear mapping is independent of the choice of the ordered basis.

Theorem 5.4. *Let V be an n-dimensional vector space with ordered basis β. Then the characteristic polynomial of the linear operator T does not depend on the chosen basis. That is, if α is another ordered basis for V, the characteristic polynomial of T is also the characteristic polynomial of $[T]_\alpha$.*

Proof Sketch. Recall: If $\beta = \{v_1, \ldots, v_n\}$ is an ordered basis of an n-dimensional vector space V, then

$$[T]_\beta = \begin{bmatrix} [T(v_1)]_\beta & [T(v_2)]_\beta & \cdots & [T(v_n)]_\beta \end{bmatrix} \in M_{n\times n}(\mathbb{F}).$$

If α is another ordered basis of V, then

$$[T]_\beta = Q^{-1}[T]_\alpha Q,$$

where Q is the change of coordinate matrix that changes β-coordinates into α-coordinates,

$$Q = [I_V]_\beta^\alpha = \begin{bmatrix} [v_1]_\alpha & [v_2]_\alpha & \cdots & [v_n]_\alpha \end{bmatrix}.$$

That means $[T]_\beta$ is similar to $[T]_\alpha$. By Theorem 5.2, $[T]_\beta$ and $[T]_\alpha$ have the same characteristic polynomial. Therefore, the characteristic polynomial of the linear operator T does not depend on the chosen basis. □

Now we will study a special type of linear mappings on a finite-dimensional vector space V and a special type of square matrices.

Definition 43.

- *A linear operator T on a finite-dimensional vector space V is called diagonalizable if there is an ordered basis β for V such that $[T]_\beta$ is a diagonal matrix.*
- *A square matrix A is called diagonalizable if L_A is diagonalizable.*

Theorem 5.5. *Let $T : V \to V$ be a linear operator on an n-dimensional vector space V. Then T is diagonalizable if and only if there is an ordered basis β for V consisting of eigenvectors of T. Moreover, if T is diagonalizable and $\beta = \{v_1, \ldots, v_n\}$ is an ordered basis for V consisting of eigenvectors of T, then the diagonal entries of $[T]_\beta$ are eigenvalues of T corresponding to the eigenvectors v_k's, $k = 1, \ldots, n$.*

Proof. ($\Rightarrow$) Suppose T is diagonalizable. By definition, there exists an ordered basis $\beta = \{v_1, \ldots, v_n\}$ for V such that $[T]_\beta$ is diagonal. That is

$$\begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} = [T]_\beta = \begin{bmatrix} [T(v_1)]_\beta & [T(v_2)]_\beta & \cdots & [T(v_n)]_\beta \end{bmatrix}.$$

Therefore, for all $1 \le k \le n$, $[T(v_k)]_\beta = [0, \ldots, 0, \lambda_k, 0, \ldots, 0]^T$, whose the k-th entry is λ_k and other entries are zero. By the definition of coordinate vectors,

$$T(v_k) = \lambda_k v_k, \quad \forall 1 \le k \le n.$$

Since v_k is an element in a basis of V, $v_k \neq 0$. Hence, (λ_k, v_k) is an eigenpair of T, $\forall 1 \le k \le n$ and $\beta = \{v_1, \ldots, v_n\}$ is a basis for V consisting of eigenvectors of T.

($\Leftarrow$) Conversely, suppose V has an ordered basis $\beta = \{v_1, \ldots, v_n\}$ of eigenvectors of T. Then, there are scalars $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ such that

$$T(v_k) = \lambda_k v_k, \quad \forall 1 \leq k \leq n.$$

Hence, $[T(v_k)]_\beta = \lambda_k e_k, \ \forall 1 \leq k \leq n$, and

$$[T]_\beta = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix}.$$

□

Notation: For a diagonal matrix $D = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{bmatrix} \in M_{n\times n}(\mathbb{F})$, we also write $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.

Below is the version of Theorem 5.5 for the linear operator $L_A : \mathbb{F}^n \to \mathbb{F}^n$, where $A \in M_{n\times n}(\mathbb{F})$. Note that eigenvectors of the linear operator L_A are eigenvectors of the matrix A.

Theorem 5.6. *Let $A \in M_{n\times n}(\mathbb{F})$. Then A is diagonalizable if and only if there is an ordered basis β for $\mathbb{F}^n$ consisting of eigenvectors of A. Moreover, if A is diagonalizable and β is an ordered basis for $\mathbb{F}^n$ consisting of eigenvectors of A, then $[L_A]_\beta$ is diagonal whose diagonal entries are eigenvalues of A corresponding to the vectors in β.*

Example 55. Recall to the previous example. The matrix $A = \begin{bmatrix} -1 & 6 & 3 \\ 1 & 0 & -1 \\ -3 & 6 & 5 \end{bmatrix}$ has two eigenvalues $\lambda_1 = 0$ and $\lambda_2 = 2$. A basis for E_{λ_1} is $\left\{ v_1 = \begin{bmatrix} 3 \\ -1 \\ 3 \end{bmatrix} \right\}$ and a basis for E_{λ_2} is $\left\{ v_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}, v_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\}$. We can verify that $\{v_1, v_2, v_3\}$ is linearly independent (check this!). Since $\dim(\mathbb{F}^3) = 3$, $\{v_1, v_2, v_3\}$ is a basis for $\mathbb{F}^3$. Hence, A is diagonalizable.

Finally, to conclude this section, we study a very important property of diagonalizable matrices.

Theorem 5.7 (Diagonalizable Matrices)**.** *Let $A \in M_{n\times n}(\mathbb{F})$. Then A is diagonalizable if and only if there exist an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$.*

Proof Sketch. Let $\{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{F}^n$. For any matrix $B = [b_1 \ldots b_n] \in M_{m\times n}(\mathbb{F})$ whose column vectors are $b_1, \ldots, b_n$ and any diagonal matrix $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n) \in M_{n\times n}(\mathbb{F})$, we have

$$B \operatorname{diag}(\lambda_1, \ldots, \lambda_n) = B[\lambda_1 e_1 \ldots \lambda_n e_n] = [B(\lambda_1 e_1) \ldots B(\lambda_n e_n)] = [\lambda_1 B e_1 \ldots \lambda_n B e_n] = [\lambda_1 b_1 \ldots \lambda_n b_n].$$

Then

A is diagonalizable $\Leftrightarrow \exists$ a basis $\beta = \{v_1, \ldots, v_n\}$ for $\mathbb{F}^n$ of eigenvectors of A (by Theorem 5.6)

$\Leftrightarrow \exists$ a basis $\beta = \{v_1, \ldots, v_n\}$ for $\mathbb{F}^n$ and scalars $\lambda_1, \ldots, \lambda_n$ s.t. $Av_k = \lambda_k v_k$, $\forall 1 \leq k \leq n$.

$\Leftrightarrow \exists$ a basis $\beta = \{v_1, \ldots, v_n\}$ for $\mathbb{F}^n$ and scalars $\lambda_1, \ldots, \lambda_n$ s.t. $[Av_1 \ldots Av_n] = [\lambda_1 v_1 \ldots \lambda_n v_n]$

$\Leftrightarrow \exists$ an invertible matrix $P = [v_1 \ldots v_n]$ and $\exists$ a diagonal matrix $D = \text{diag}(\lambda_1, \ldots, \lambda_n)$ s.t. $AP = PD$.

$\Leftrightarrow \exists$ an invertible matrix P and $\exists$ a diagonal matrix D s.t. $P^{-1}AP = D$.

□

Remark 26.

1. From the proof of Theorem 5.7, if there exist an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$, then the columns of P are eigenvectors of A and the diagonal entries of D are the eigenvalues of A corresponding to the columns of P. Note that the factorization $A = PDP^{-1}$, where P is invertible and D is diagonal, if exists, is not unique. Even if we sort the diagonal entries of D in a given order (such as decreasing or increasing order), D is then unique, but P is still not unique.

2. If $A \in M_{n\times n}(\mathbb{F})$ is diagonalizable, there exist an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$. Then $A = PDP^{-1}$ and by induction, we can prove that

$$A^2 = (PDP^{-1})(PDP^{-1}) = PDP^{-1}PDP^{-1} = PD^2P^{-1}, \ldots, A^m = PD^mP^{-1}, \ \forall m = 1, 2, \ldots$$

Note that if $D = \text{diag}(\lambda_1, \ldots, \lambda_n)$ then $D^m = \text{diag}(\lambda_1^m, \ldots, \lambda_n^m)$ for all $m = 1, 2, \ldots$. Therefore, if A is diagonalizable, we can factorize A and compute A^m based on the eigenvectors and eigenvalues of A.

For example, the matrix $A = \begin{bmatrix} 0.9 & 0.7 \\ 0.1 & 0.3 \end{bmatrix} \in M_{2\times 2}(\mathbb{R})$ has two eigenvalues $\lambda_1 = 1$ and $\lambda_2 = \frac{1}{5}$. A basis for E_{λ_1} is $v_1 = (7, 1)^T$ and a basis for E_{λ_2} is $v_2 = (-1, 1)^T$. Since v_1 is not a scalar multiple of v_2, the set $\{v_1, v_2\}$ is linearly independent and thus a basis for $\mathbb{R}^2$. Hence A is diagonalizable. Let

$$P = [v_1 \ v_2] = \begin{bmatrix} 7 & -1 \\ 1 & 1 \end{bmatrix} \quad D = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{5} \end{bmatrix}.$$

Then $A = PDP^{-1}$. Therefore,

$$\begin{aligned} A^{2021} &= (PDP^{-1})(PDP^{-1}) \ldots (PDP^{-1}) \\ &= PD^{2021}P^{-1} \\ &= \begin{bmatrix} 7 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{5^{2021}} \end{bmatrix} \left(\begin{bmatrix} 7 & -1 \\ 1 & 1 \end{bmatrix} \right)^{-1} \\ &= \begin{bmatrix} 7 & -5^{-2021} \\ 1 & 5^{-2021} \end{bmatrix} \left(\frac{1}{8} \begin{bmatrix} 1 & 1 \\ -1 & 7 \end{bmatrix} \right) \\ &= \frac{1}{8} \begin{bmatrix} 7 + 5^{-2021} & 7 - 7(5^{-2021}) \\ 1 - 5^{-2021} & 1 + 7(5^{-2021}) \end{bmatrix}. \end{aligned}$$

Week 12.

In previous lectures, we know that all eigenvalues of a given matrix $A \in M_{n\times n}(\mathbb{F})$ are roots of its characteristic polynomial $p_A(t) = \det(A - tI_n)$. From each eigenvalue, we have a corresponding eigenspace. We also know that every eigenvector of A belongs to some eigenspace of A. Now we will study further the relation among eigenspaces of a given matrix (or of a linear mapping from a finite dimensional vector space to itself) and the connection between eigenspaces and the characteristic polynomial.

Theorem 5.8. *Let V be a vector space and $T : V \to V$ be linear. Let $v_1, \ldots, v_k$ be eigenvectors of T, with eigenvalues $\lambda_1, \ldots, \lambda_k$, respectively. Assume that these eigenvalues are distinct, i.e.,*

$$\lambda_i \neq \lambda_j \quad \text{if} \quad i \neq j.$$

Then $E_i \cap E_j = \{0\}$ for all $1 \leq i \neq j \leq k$ and $\{v_1, \ldots, v_k\}$ is linearly independent.

Proof. Fix $i \neq j$. Let $v \in E_i \cap E_j$. Then $\lambda_i v = T(v) = \lambda_j v$. So, $(\lambda_i - \lambda_j)v = 0$. Since $(\lambda_i - \lambda_j) \neq 0$, $v = 0$. Therefore, $E_i \cap E_j = \{0\}$.

We will prove the second statement by induction on k. For $k = 1$, since v_1 is an eigenvector of T, $v_1 \neq 0$, so $\{v_1\}$ is linearly independent. Assume $k > 1$ and the theorem holds for any set of $(k-1)$ eigenvectors corresponding to $(k-1)$ distinct eigenvalues. Suppose we have a relation

$$c_1 v_1 + \cdots + c_{k-1} v_{k-1} + c_k v_k = 0, \tag{4}$$

where $v_1, \ldots, v_k$ are eigenvectors of T corresponding to the distinct eigenvalues $\lambda_1, \ldots, \lambda_k$ and $c_1, \ldots, c_k \in \mathbb{F}$. Applying T to both sides of Equation (4) and substituting $T(v_j) = \lambda_j v_j$, $1 \leq j \leq k$, we have

$$c_1\lambda_1 v_1 + \cdots + c_{k-1}\lambda_{k-1} v_{k-1} + c_k\lambda_k v_k = 0.$$

We multiply both sides of Equation (4) by λ_k to obtain

$$\lambda_k c_1 v_1 + \cdots + \lambda_k c_{k-1} v_{k-1} + \lambda_k c_k v_k = 0.$$

Subtracting the last two equations yields

$$c_1(\lambda_1 - \lambda_k)v_1 + \cdots + c_{k-1}(\lambda_{k-1} - \lambda_k)v_{k-1} = 0.$$

By the induction hypothesis, $\{v_1, \ldots, v_{k-1}\}$ is linearly independent. Therefore,

$$c_1(\lambda_1 - \lambda_k) = c_2(\lambda_2 - \lambda_k) = c_{k-1}(\lambda_{k-1} - \lambda_k) = 0.$$

Since $\lambda_j - \lambda_k \neq 0$ for $j = 1, \ldots, k-1$, we conclude that

$$c_1 = \cdots = c_{k-1} = 0.$$

Therefore, Equation (4) reduces to $c_k v_k = 0$, which leads to $c_k = 0$ since $v_k \neq 0$. Consequently, $c_1 = \cdots = c_k = 0$, and it follows that $\{v_1, \ldots, v_k\}$ is linearly independent. □

Corollary 5.8.1. *1. Let $T : V \to V$ be linear on an n-dimensional vector space V. If T has n distinct eigenvalues, then T is diagonalizable.*

2. Let $A \in M_{n\times n}(\mathbb{F})$. If A has n distinct eigenvalues, A is diagonalizable.

Proof. 1. Suppose T has n distinct eigenvalues $\lambda_1, \ldots, \lambda_n$. For each eigenvalue λ_i, choose an eigenvector v_i. By Theorem 5.8, $\{v_1, \ldots, v_n\}$ is linearly independent. Since $\dim(V) = n$, the set $\{v_1, \ldots, v_n\}$ is a basis for V. Therefore, T is diagonalizable.
2. For a matrix $A \in M_{n\times n}(\mathbb{F})$, eigenvalues of A are eigenvalues of the linear mapping L_A and eigenvectors of A are eigenvectors of L_A, and vice versa. Hence, we have the matrix version of part 1. □

Remark 27. The converse of Corollary 5.8.1 is not true. That is, there exists a linear transformation T from an n-dimensional vector space to itself such that T is diagonalizable but T does not have n distinct eigenvalues. For example, the identity matrix is diagonalizable,

$$I_n = P^{-1} I_n P, \quad \text{for any invertible matrix } P,$$

even though I_n has only one eigenvalue $\lambda = 1$ (check this).

Example 56. 1. Let V be the vector space consisting of all differentiable functions of a real variable x and $T : V \to V$ defined by $T(f(x)) = f'(x)$. We proved that T is linear. Let $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ be distinct numbers. The functions

$$e^{\lambda_1 x}, \ldots, e^{\lambda_k x}$$

are eigenvectors of T corresponding to the eigenvalues $\lambda_1, \ldots, \lambda_k$, respectively. By Theorem 5.8, $\{e^{\lambda_1 x}, \ldots, e^{\lambda_k x}\}$ is linearly independent.

2. The matrix $A = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$ has two distinct eigenvalues $\lambda_1 = -1$ and $\lambda_2 = 4$. By Corollary 5.8.1, the matrix A is diagonalizable.

Now, we will extend Theorem 5.8 to the case where for each eigenvalue λ_i from the set of distinct eigenvalues $\{\lambda_1, \ldots, \lambda_k\}$, instead of choosing one eigenvector in the corresponding eigenspace, we choose a finite set of linearly independent vectors in that eigenspace. Then the union of those sets is still a linearly independent set. It is stated as follows.

Theorem 5.9. *Let $T : V \to V$ be linear and let $\lambda_1, \ldots, \lambda_k$ be distinct eigenvalues of T. For each $j = 1, 2, \ldots, k$, let S_j be a finite linearly independent subset of the eigenspace E_{λ_j}. Then*

1. $S_i \cap S_j = \varnothing$, $\forall 1 \le i \ne j \le k$.

2. The set $S = S_1 \cup S_2 \cup \cdots S_k$ is a linearly independent subset of V and $|S| = \sum_{i=1}^{k} |S_i|$.

Proof. 1. Since, for each $i \in \{1, \ldots, k\}$, S_i is linearly independent, $S_i \subseteq E_{\lambda_i} - \{0\}$. In addition, since $E_{\lambda_i} \cap E_{\lambda_j} = \{0\}$, we have $S_i \cap S_j = \varnothing$, $\forall 1 \le i \ne j \le k$.

2. Therefore, $|S| = |S_1 \cup S_2 \cup \cdots S_k| = \sum_{i=1}^{k} |S_i|$.

Suppose $S_i = \{v_{i,1}, \ldots, v_{i,n_i}\} \subseteq E_{\lambda_i}$, for $1 \leq i \leq k$. Then,

$$S = \{v_{i,j} \mid 1 \leq i \leq k, 1 \leq j \leq n_i\}.$$

Consider any scalars $\{a_{ij}\}$ such that

$$\sum_{i=1}^{k} \sum_{j=1}^{n_i} a_{ij} v_{i,j} = 0.$$

Let $w_i = \sum_{j=1}^{n_i} a_{ij} v_{i,j}$. Then

$$w_1 + \cdots + w_k = 0. \tag{5}$$

Since E_{λ_i} is a vector space and $v_{i,j} \in E_{\lambda_i}$, $\forall 1 \leq j \leq n_i$, we have $w_i \in E_{\lambda_i}$. Hence, w_i is either the zero vector or an eigenvector of T corresponding to the eigenvalue λ_i. There are two cases:

- Case 1: $w_i = 0, \forall 1 \leq i \leq k$. Then for each fixed $i \in \{1, \ldots, k\}$, we have $0 = w_i = \sum_{j=1}^{n_i} a_{ij} v_{i,j} = 0$. Since $\{v_{i,1}, \ldots, v_{i,n_i}\}$ is linearly independent, $a_{i,j} = 0$ for all $1 \leq j \leq n_i$. So $a_{ij} = 0$ for all $1 \leq i \leq k$ and for all $1 \leq j \leq n_i$.

- Case 2: There exists $1 \leq i \leq k$ such that $w_i \neq 0$. By renumbering if necessary, suppose that, $w_i \neq 0$ for all $1 \leq i \leq m$, and $w_i = 0$ for $m < i \leq k$. That is, $w_1, \ldots, w_m$ are eigenvectors of T corresponding to the eigenvalues $\lambda_1, \ldots, \lambda_m$, and $w_{m+1} = \cdots = w_k = 0$. Equation (5) becomes $w_1 + \cdots + w_m = 0$, which implies $\{w_1, \ldots, w_m\}$ is linearly dependent. On the other hand, since $w_1, \ldots w_m$ are eigenvectors of T corresponding to the distinct eigenvalues $\lambda_1, \ldots, \lambda_m$, by Theorem 5.8, $\{w_1, \ldots, w_m\}$ is linearly independent, a contradiction. Therefore case 2 can't happen.

In conclusion, we must have $w_1 = \ldots = w_k = 0$ and $a_{i,j} = 0$ for all $1 \leq i \leq k, 1 \leq j \leq n_i$. Thus, S is linearly independent.

□

We also study diagonalizable matrices and its equivalent conditions, which provide some interesting insights about the importance of diagonalizable matrices. However, all those conditions are not constructive. That is, given a square matrix $A \in M_{n\times n}(\mathbb{F})$, we would like to have a constructive algorithm to classify A diagonalizable or not and to construct explicitly a basis for $\mathbb{F}^n$ of eigenvectors of A if exsits. We will answer these questions today, using characteristic polynomials and properties of eigenspaces.

Definition 44. *A polynomial $f(t) \in \mathbb{F}[t]$ splits over $\mathbb{F}$ if there are scalars $c, a_1, \ldots, a_n$ (not necessarily distinct) in $\mathbb{F}$ such that*

$$f(t) = c(t - a_1)(t - a_2) \cdots (t - a_n).$$

Example 57. Consider $f(t) = t^3 + t^2 + t + 1 = (t^2 + 1)(t + 1)$.

- $f(t)$ does not split over $\mathbb{R}$, $\mathbb{Q}$.
- $f(t)$ splits over $\mathbb{C}$: $f(t) = (t + i)(t - i)(t + 1)$.
- $f(t)$ splits over $\mathbb{F}_2$: $f(t) = (t + 1)(t + 1)(t + 1)$.

Theorem 5.10. *Let V be a finite-dimensional vector space. The characteristic polynomial of any diagonalizable linear transformation $T : V \to V$ splits.*

Proof. Let T be a diagonalizable linear operator on an n-dimensional vector space V. Then there exists an ordered basis β of V so that $[T]_\beta$ is a diagonal matrix D. Then the characteristic polynomial of T is

$$p_D(t) = (\lambda_1 - t)\dots(\lambda_n - t) = (-1)^n(t - \lambda_1)\dots(t - \lambda_n),$$

which splits over $\mathbb{F}$. □

Question: Conversely, if the characteristic polynomial of a linear transformation $T : V \to V$ on the finite-dimensional vector space V splits, is T diagonalizable? The answer is NO, in general. Here is an example. Consider $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$. Its characteristic polynomial is $p_A(t) = (1-t)^2$. Therefore, $p_A(t)$ splits. Also, A has only one eigenvalue $\lambda = 1$. We can check that (prove this!) a basis for E_λ is $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$. Therefore, A is not diagonalizable.

That means besides a split characteristic polynomial, we need additional requirement(s) to guarantee a linear transformation $T : V \to V$ diagonalizable, where $\dim(V) < \infty$. It involves algebraic and geometric multiplicities of eigenvalues.

Definition 45. *Let V be a finite dimensional vector space and $T : V \to V$ be linear. Let λ be an eigenvalue of T and $p(t)$ be the characteristic polynomial of T.*

- *The algebraic multiplicity of λ is the largest positive integer k for which $(t - \lambda)^k$ is a factor of $p(t)$.*
- *The geometric multiplicity of λ is the dimension of the eigenspace E_λ.*

For example, in Example 53, the matrix A has two eigenvalues 0 and 2. For $\lambda_1 = 0$, its algebraic multiplicity is 1 and its geometric mutliplicity is 1. For $\lambda_2 = 2$, its algebraic multiplicity is 2 and its geometric mutliplicity is 2.

From Remark 22, we know that $1 \le \dim(E_\lambda) \le \dim(V)$. Now we prove a stronger result, which says that the geometric multiplicity of any eigenvalue, $\dim(E_\lambda)$, is always smaller or equal than the algebraic multiplicity of that eigenvalue.

Theorem 5.11. *Let $T : V \to V$ be a linear transformation from a finite dimensional vector space V to itself and let λ be an eigenvalue of T having algebraic multiplicity m_λ. Then $1 \le \dim(E_\lambda) \le m_\lambda$.*

Proof Sketch. Let $n = \dim(V)$. Suppose $\dim(E_\lambda) = k$. Then $k \le n$. Choose an ordered basis $\{v_1, \dots, v_k\}$ for E_λ and extend it to an ordered basis $\beta = \{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ for V.

Let $A = [T]_\beta$. Then $p(t) = p_A(t)$. For each $1 \le j \le k$, since $T(v_j) = \lambda v_j$, $[T(v_j)]_\beta = \lambda e_j$, where e_j is the j-th vector in the standard basis for $\mathbb{F}^n$. Therefore,

$$A = [T]_\beta = \left[[T(v_1)]_\beta, \ \cdots, [T(v_k)]_\beta, \ [T(v_{k+1})]_\beta, \cdots, \ [T(v_n)]_\beta \right] = \begin{bmatrix} \lambda I_k & B \\ 0 & C \end{bmatrix}.$$

Using results in Assignment 8 Question 3, we have

$$p(t) = \det(A - tI_n) = \det \begin{bmatrix} (\lambda - t)I_k & B \\ 0 & C - tI_{n-k} \end{bmatrix} = \det((\lambda - t)I_k) \det(C - tI_{n-k}) = (\lambda - t)^k \det(C - tI_{n-k}).$$

Since $\det(C - tI_{n-k})$ is a polynomial of degree $(n-k) \geq 0$, $(\lambda - t)^k$ is a factor of $p(t)$, therefore, $k \leq m_\lambda$, which completes the proof. □

Now we are ready to discuss a constructive algorithm where we can classify all square matrices "to be or not to be" diagonalizable. This theorem also provides an explicit algorithm to construct a basis for a finite-dimensional vector space V consisting of eigenvectors of T, if T is diagonalizable.

Theorem 5.12. *Let $T : V \to V$ be a linear transformation on a finite dimensional vector space V. Let $\lambda_1, \ldots, \lambda_k$ be all distinct eigenvalues of T and let $m_1, \ldots, m_k$ be their multiplicities. Then T is diagonalizable iff*

1. *$p_T(t)$ splits, i.e., $p_T(t) = (-1)^n(t - \lambda_1)^{m_1} \ldots (t - \lambda_k)^{m_k}$, and*
2. *For each $i = 1, \ldots, k$, $\dim(E_{\lambda_i}) = m_i$.*

Proof. ($\Leftarrow$) Assume (1) and (2) holds. So $\sum_{i=1}^{k} m_i = \deg(p_T(t)) = \dim(V)$.

- Let S_i be a basis for E_{λ_i}, then S_i has m_i elements which are eigenvectors of T corresponding to eigenvalue λ_i.
- By Theorem 5.9, the set $S = \bigcup_{i=1}^{k} S_i$ is linearly independent and S has $\sum_{i=1}^{k} m_i = \dim(V)$ elements. So S is a basis for V of eigenvectors of T.

($\Rightarrow$) Suppose T is diagonalizable. By Theorem 5.5, there is an ordered basis β for V of eigenvectors of T. By Theorem 5.10, $p_T(t)$ splits. Let $S_i = \beta \cap E_{\lambda_i}$.

- Since β is a set of eigenvectors, $\beta \subset \bigcup_{i=1}^{k} E_{\lambda_i}$. Therefore,

  $$\beta = \beta \cap \bigcup_{i=1}^{k} E_{\lambda_i} = \bigcup_{i=1}^{k} (\beta \cap E_{\lambda_i}) = \bigcup_{i=1}^{k} S_i.$$

  Hence, $\dim(V) = |\beta| = \left| \bigcup_{i=1}^{k} S_i \right|$. In addition, for every pair (i, j) s.t. $1 \leq i \neq j \leq k$, since $E_{\lambda_i} \cap E_{\lambda_j} = \{0\}$ and $0 \notin \beta$, we have $S_i \cap S_j = \varnothing$. Therefore, $\left| \bigcup_{i=1}^{k} S_i \right| = \sum_{i=1}^{k} |S_i|$.

  Thus, $\dim(V) = \sum_{i=1}^{k} |S_i|$.
- On the other hand, since $S_i = \beta \cap E_{\lambda_i}$, S_i is a linearly independent subset of E_{λ_i}. Therefore, $|S_i| \leq \dim(E_{\lambda_i}) \leq m_i$. Hence, $\sum_{i=1}^{k} |S_i| \leq \sum_{i=1}^{k} m_i = \dim(V)$. The equality holds iff $|S_i| = \dim(E_{\lambda_i}) = m_i$ for all $1 \leq i \leq k$, which completes the proof.

□

Remark 28. The above proof provides a procedure to check whethere a square matrix is diagonalizable or not. If yes, it provides the factorization of A as PDP^{-1} where D is a diagonal matrix.

Step 1: Compute its characterstic polynomial $p_A(t)$. If $p_A(t)$ does not split, A is not diagonalizable. Otherwise, go to Step 2.

Step 2: Find all eigenvalues of A. Suppose $\lambda_1, \ldots, \lambda_k$ are all distinct eigenvalues of A and m_j is the algebraic multiplicity of λ_j, for $1 \leq j \leq k$.

Step 3: Find a basis for each eigenspace E_{λ_j}, for $1 \leq j \leq k$.

Case 1: If there exists $1 \leq j \leq k$ such that $\dim E_{\lambda_j} \neq m_j$, the matrix A is not diagonalizable.

Case 2: If $m_j = \dim E_{\lambda_j}$ for all $1 \leq j \leq k$, the matrix A is diagonalizable. Let $\beta = \beta_1 \cup \beta_2 \cup \cdots \cup \beta_k$, where β_j is an ordered basis for E_{λ_j}, for $1 \leq j \leq k$. Then β is a basis for V.

Let P be a square matrix whose columns are vectors from β and let D be a diagonal matrix whose diagonal entries are eigenvalues of A corresponding to the column of P. Then

$$A = PDP^{-1}.$$

In addition,

$$A^m = (PDP^{-1})(PDP^{-1})\cdots(PDP^{-1}) = PD^mP^{-1}, \quad \forall m \geq 1.$$

Note that if $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, then $D^m = \operatorname{diag}(\lambda_1^m, \ldots, \lambda_n^m)$, for all $m \geq 1$.

Example 58. Check whether $A = \begin{bmatrix} -2 & 1 & 1 \\ -1 & 0 & 1 \\ -2 & 2 & 1 \end{bmatrix}$ is diagonalizable. If yes, find an invertible matrix P and a diagonal matrix D such that $P^{-1}AP = D$. Also, find A^{100}.

Answer. Exercise. □

To conclude this course, we will study the Cayley-Hamilton theorem.

Definition 46. *Let $A \in M_{n\times n}(\mathbb{F})$ and $f(t) = a_N t^N + \cdots + a_1 t + a_0 \in \mathbb{F}[t]$. Define*

$$f(A) := a_N A^N + \cdots + a_1 A + a_0 I_n.$$

Thus $f(A) \in M_{n\times n}(\mathbb{F})$.

Lemma 15. *Let $f, g \in \mathbb{F}[t]$ and $A \in M_{n\times n}(\mathbb{F})$. Recall that $(fg)(t) := f(t)g(t) \in \mathbb{F}[t]$. Then*

$$\begin{aligned}(f+g)(A) &= f(A) + g(A),\\ (cf)(A) &= cf(A), \quad \text{for} \quad c \in \mathbb{F},\\ (fg)(A) &= f(A)g(A),\\ f(A)g(A) &= g(A)f(A).\end{aligned}$$

Proof Sketch. The equality $f(A)g(A) = g(A)f(A)$ can be derived by expanding and using $A^i\ A^j = A^j\ A^i$. □

Example 59. Let $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$. Consider $A \in M_{n\times n}(\mathbb{F})$ and

$$f(t) = (t-\alpha_1)\ldots(t-\alpha_k) = (f_1 \ldots f_k)(t) \in \mathbb{F}[t],$$

where $f_i(t) = t - \alpha_i$. Then $f_i(A) = A - \alpha_i I_n$ and by Lemma 15

$$f(A) = f_1(A)\ldots f_k(A) = (A-\alpha_1 I_n)\ldots(A-\alpha_k I_n).$$

Using the laws of addition and multiplication, we can prove the following result for square matrices.

Lemma 16. *Suppose $A \in M_{n\times n}(\mathbb{F})$. Then there exists a non-zero polynomial $f \in \mathbb{F}[t]$ such that $f(A) = 0$.*

Proof. Consider the set of matrices $S = \{I_n, A, A^2, \ldots, A^{n^2}\} \subset M_{n\times n}(\mathbb{F})$. Since $\dim(M_{n\times n}(\mathbb{F}) = n^2$ and S has (n^2+1) matrices, S is linearly dependent. So there exist $a_0, a_1, \ldots, a_{n^2} \in \mathbb{F}$, not all 0, such that

$$a_0 I_n + a_1 A + a_2 A^2 + \cdots + a_{n^2} A^{n^2} = 0.$$

Let $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{n^2} t^{n^2} \in \mathbb{F}[t]$. Then $f(A) = 0$. □

Now, for each given $A \in M_{n\times n}(\mathbb{F})$, we will determine a polynomial $P(t)$, which can be constructed explicitly, such that $P(A) = 0$. The proof needs to use the property that every polynomial has a root, which leads to the following requirement on the scalar field $\mathbb{F}$.

Definition 47. *A field $\mathbb{F}$ is called algebraically closed if every polynomial in $\mathbb{F}[t]$ of degree ≥ 1 has a root in $\mathbb{F}$.*

For example, the set of complex numbers, $\mathbb{C}$, is algebraically closed by the Fundamental Theorem of Algebra. However, the set of real numbers $\mathbb{R}$ is not algebraically closed, since $x^2+1 \in \mathbb{R}[x]$ does not have a root in $\mathbb{R}$.

Theorem 5.13 (Cayley-Hamilton Theorem)**.** *Let $\mathbb{F}$ be algebraically closed. For every $A \in M_{n\times n}(\mathbb{F})$, we have $p_A(A) = 0$, where $p_A(t)$ is the characteristic polynomial of A.*

In order to prove the Cayley-Hamilton theorem, we first need to prove the following result.

Theorem 5.14. *Let $\mathbb{F}$ be algebraically closed. Every $A \in M_{n\times n}(\mathbb{F})$ is similar to an upper-triangular matrix.*

Sketch Proof of Theorem 5.14. It suffices to build an ordered basis $\beta = \{v_1, \ldots, v_n\}$ for $\mathbb{F}^n$ such that

$$Av_i \in \text{span}\,(v_1, v_2, \ldots, v_i), \quad \text{for all} \quad 1 \le i \le n.$$

To prove the existence of β, it is enough to show that if $1 \le i \le n$ and $\{v_1, \ldots, v_{i-1}\}$ is linearly independent in $\mathbb{F}^n$, there exists $v_i \in \mathbb{F}^n$ such that

1. $v_i \notin \text{span}(\{v_1, \ldots, v_{i-1}\})$, and
2. $Av_i \in \text{span}(\{v_1, \ldots, v_i\})$.

Case 1: i=1. Since $p_A(t) \in \mathbb{F}[t]$ and $\mathbb{F}$ is algebraically closed, $p_A(t)$ has a solution $\lambda_1 \in \mathbb{F}$. Then λ_1 is an eigenvalue of A. Let v_1 be an eigenvector of A corresponding to the eigenvalue λ_1. Then $Av_1 = \lambda_1 v_1 \in \text{span}(v_1)$.

Case 2: $n \ge i > 1$. Then $V \setminus \text{span}(\{v_1, \ldots, v_{i-1}\}) \neq \varnothing$. Fix $x \in V \setminus \text{span}(\{v_1, \ldots, v_{i-1}\})$. Consider

$$\mathcal{S} = \{g \in \mathbb{F}[t] : g \neq 0, \text{ and } g(A)x \in \text{span}(\{v_1, \ldots, v_{i-1}\})\}.$$

By Lemma 16, there exists a nonzero polynomial $f \in \mathbb{F}[t]$ such that $f(A) = 0$. Hence

$$f(A)x = 0 \in \text{span}(\{v_1, \ldots, v_{i-1}\}).$$

So $f \in \mathcal{S}$. In other words, $\mathcal{S} \neq \varnothing$. Let $g \in \mathcal{S}$ be a polynomial in $\mathcal{S}$ of smallest degree. Then $\deg(g) \ge 1$ (prove this). Since $\mathbb{F}$ is algebraically closed and $g \in \mathbb{F}[t]$, g has a root $c \in \mathbb{F}$ and

$$g(t) = (t - c)h(t), \quad \text{for some} \quad h \in \mathbb{F}[t] - \{0\}.$$

Since $\deg(h) < \deg(g)$, $h \notin \mathcal{S}$. Combining with $h \neq 0$, we have $h(A)x \notin \text{span}(\{v_1, \ldots, v_{i-1}\})$. Let $v_i = h(A)x$. Then

$$Av_i - cv_i = (A - cI_n)v_i = (A - cI_n)(h(A)x) = ((A - cI_n)h(A))x = g(A)x \in \text{span}(\{v_1, \ldots, v_{i-1}\}).$$

Therefore, $Av_i \in \text{span}(\{v_1, \ldots, v_{i-1}, v_i\})$, which completes the proof. □

Let's proof the Cayley-Hamilton Theorem. We first prove the Cayley-Hamilton theorem for an upper triangular matrix A. Suppose

$$A = \begin{pmatrix} c_1 & * & \cdots & * & * \\ 0 & c_2 & \cdots & * & * \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & c_{n-1} & * \\ 0 & 0 & \cdots & 0 & c_n \end{pmatrix}.$$

Therefore,

$$p_A(t) = (-1)^n(t-c_1)(t-c_2)\dots(t-c_{n-1})(t-c_n).$$

Hence

$$p_A(A) = (-1)^n(A-c_1I_n)(A-c_2I_n)\cdots(A-c_{n-1}I_n)(A-c_nI_n).$$

To prove $p_A(A)=0$, we will first prove that $p_A(A)x=0$ for all $x\in\mathbb{F}^n$. Then by the matrix equality theorem, $p_A(A)=0$. Let $x\in\mathbb{F}^n$. Then

$$(A-c_nI_n)x = \begin{pmatrix} c_1 & * & \cdots & * & * \\ 0 & c_2 & \cdots & * & * \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & c_{n-1} & * \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} x = \begin{pmatrix} * \\ * \\ \vdots \\ * \\ 0 \end{pmatrix} := x^{(1)}.$$

Then

$$(A-c_{n-1}I_n)(A-c_nI_n)x = (A-c_{n-1}I_n)x^{(1)} = \begin{pmatrix} c_1 & * & \cdots & * & * \\ 0 & c_2 & \cdots & * & * \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & * \\ 0 & 0 & \cdots & 0 & * \end{pmatrix} \begin{pmatrix} * \\ * \\ \vdots \\ * \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ * \\ \vdots \\ 0 \\ 0 \end{pmatrix} := x^{(2)}.$$

Continuing this process, we obtain

$$(A-c_1I_n)(A-c_2I_n)\cdots(A-c_{n-1}I_n)(A-c_nI_n)x = 0.$$

That is $p_A(A)x=0$ for all $x\in\mathbb{F}^n$. So $p_A(A)=0$.

For general matrix $A\in M_{n\times n}(\mathbb{F})$, by Theorem 5.14, A is similar to an upper triangular matrix U. Then $A=QUQ^{-1}$ for some invertible matrix P. Then

$$p_A(A) = p_A(QUQ^{-1}) \overset{\text{(check this!)}}{=} Qp_A(U)Q^{-1} \overset{\text{Since } p_A(t)=p_U(t)}{=} Qp_U(U)Q^{-1} = QOQ^{-1} = 0.$$

Example 60. Consider

$$A = \begin{bmatrix} 1 & 6 & 3 \\ 0 & -2 & 0 \\ 3 & 6 & 1 \end{bmatrix}.$$

Its characteristic polynomial is $p_A(t) = -t^3+12t+16$. By the Cayley-Hamilton theorem,

$$-A^3+12A+16I_3 = 0.$$

Therefore, we can compute A^3 without computing the power of A,

$$A^3 = 12A+16I_3 = \begin{bmatrix} 28 & 72 & 36 \\ 0 & -8 & 0 \\ 36 & 72 & 28 \end{bmatrix}.$$

Also, from that equation, we have

$$I_3 = \frac{1}{16}(A^3-12A) = \frac{1}{16}A(A^2-12I_3).$$

Hence A is invertible. The END.