MATH 2131

Honors in Linear and Abstract Algebra I

Prof. Meng

Contents

Part One

1. Abstract Linear Spaces

1.1 Binary Operation

> **Definition 1.1.1 — Binary Operation.** A *binary operation* on a set S is a mapping of the elements of the Cartesian product $S \times S$ to S.
>
> $$f : S \times S \to S$$
> $$(x,y) \mapsto f(x,y)$$

■ **Example 1.1** A common example of a binary operation is addition on the set of natural numbers $\mathbb{N}$.

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(x,y) \mapsto x+y \tag{1.1}$$

■

> **Definition 1.1.2 — Associative Operation.** A binary operation $f : S \times S \to S$ is said to be *associative* if, for all $x,y,z \in S$,
>
> $$f(x,f(y,z)) = f(f(x,y),z)$$

■ **Example 1.2** A common example of an associative (binary) operation is addition on the set of natural numbers $\mathbb{N}$. For all $x,y,z \in \mathbb{N}$, we have $x+(y+z) = (x+y)+z$. ■

> **Definition 1.1.3 — Identifiable Operation.** A binary operation $f : S \times S \to S$ is said to be *identifiable*, or *unital*, if there exists an element $e \in S$, the *identity* or *unit element*, such that, for all $x \in S$
>
> $$f(e,x) = x = f(x,e)$$

■ **Example 1.3** A common example of an identifiable (binary) operation is multiplication on the set of natural numbers $\mathbb{N}$. The identity element is 1, and for all $x \in \mathbb{N}$, we have $x \cdot 1 = x = 1 \cdot x$. ■

Proposition 1.1.1 The identity element of an identifiable operation is unique.

Proof. Let e_1 and e_2 be two identity elements for the operation f. Then, for any element $x \in S$, we have:

$$f(x, e_1) = x = f(e_1, x)$$
$$f(x, e_2) = x = f(e_2, x)$$

Now, consider the element e_1:

$$f(e_1, e_2) = e_1$$

But since e_2 is an identity element, we also have:

$$f(e_1, e_2) = e_2$$

Therefore, we conclude that $e_1 = e_2$, proving the uniqueness of the identity element. ∎

> (R) Two-sided identity must be unique, but one-sided identities need not be.

■ **Example 1.4** ■

> **Definition 1.1.4 — Inverse Operation.** A binary operation $f : S \times S \to S$ is said to be *invertible* if, for every element $x \in S$, there exists an element $y \in S$, called the two-sided *inverse* of x, denoted as x^{-1}, such that
>
> $$f(x, y) = e = f(y, x)$$
>
> where e is the identity element of the operation.

> (R) Invertible operation exists if inverse operation exists, i.e., there exists an identity element.

■ **Example 1.5** A common example of an invertible (binary) operation is addition on the set of integers $\mathbb{Z}$. For every integer $x \in \mathbb{Z}$, there exists an integer $y = -x$ such that:

$$x + (-x) = 0 = (-x) + x \tag{1.2}$$

where 0 is the identity element for addition. ■

Proposition 1.1.2 The inverse element of an invertible operation is unique.

Proof. Let y_1 and y_2 be two inverses of an element $x \in S$. Then, by definition of inverse, we have:

$$f(x, y_1) = e = f(y_1, x)$$
$$f(x, y_2) = e = f(y_2, x)$$

Now, consider the element y_1:

$$f(y_1, x) = e$$

But since y_2 is also an inverse of x, we can substitute e with $f(x, y_2)$:

$$f(y_1, x) = f(x, y_2) = e$$

By the associativity of the operation, we can rearrange this to:

$$y_1 = f(y_1, e) = f(y_1, f(x, y_2)) = f(f(y_1, x), y_2) = f(e, y_2) = y_2$$

Thus, the inverse element is unique. ∎

Definition 1.1.5 — Commutative Operation. A binary operation $f : S \times S \to S$ is said to be *commutative* if, for all $x, y \in S$, the following holds:

$$f(x,y) = f(y,x)$$

■ **Example 1.6** A common example of a commutative operation is addition on the set of integers $\mathbb{Z}$. For all $x, y \in \mathbb{Z}$, we have:

$$x + y = y + x$$

■

Definition 1.1.6 — Distributive Operation (Harmonic Property). A binary operation $g : S \times S \to S$ is said to be *distributive* with respect to another binary operation $f : S \times S \to S$ if, for all $x, y, z \in S$, the following holds:

$$g(x, f(y,z)) = f(g(x,y), g(x,z))$$
$$g(f(y,z), x) = f(g(y,x), g(z,x))$$

■ **Example 1.7** A common example of a distributive operation is multiplication over addition on the set of integers $\mathbb{Z}$. For all $x, y, z \in \mathbb{Z}$, we have:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(y + z) \cdot x = y \cdot x + z \cdot x$$

■

1.2 Groups, Rings, Fields

Definition 1.2.1 — Monoid. A *monoid* is a set M equipped with a binary operation $f : M \times M \to M$ such that the following properties hold:
1. *Closure Property:* For all $x, y \in M$, $f(x,y) \in M$.
2. *Associative Property*
3. *Identifiable Property*

We say (M, f) is a monoid, and f is the *monoid operation* on the set M. A set M with a monoid operation f is the *monoid structure*.

Definition 1.2.2 — Group. A *group* is a set G equipped with a monoid operation $f : G \times G \to G$ with the additional property that every element has an inverse, *Invertible Property*.

■ **Example 1.8** $(\mathbb{R} \setminus \{0\}, \times)$ is a group, but $(\mathbb{R}, \times)$ is not a group since 0 does not have a multiplicative inverse.   ■

Definition 1.2.3 — Abelian Monoid / Group. A monoid / group (G, f) is said to be an *abelian monoid / group* if the monoid / group operation f is commutative, *Commutative Property*.

Definition 1.2.4 — Unital Ring. A (unital) ring is a set R equipped with two binary operations $f : R \times R \to R$ (addition) and $g : R \times R \to R$ (multiplication) such that the following properties hold:
1. *Additive Group:* (R, f) is an abelian group.
2. *Multiplicative Monoid:* (R, g) is a monoid.
3. *Distributive Property:* g with respect to f.

Definition 1.2.5 — Commutative Ring. A *commutative ring* is a unital ring R such that the multiplication operation $g : R \times R \to R$ is commutative.

■ **Example 1.9** $(\mathbb{Z}, +, \times)$ is a unital commutative ring.   ■

Definition 1.2.6 — Field. A *field* is a unital commutative ring F such that every non-zero element has a multiplicative inverse.

■ **Example 1.10** $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are fields.   ■

■ **Example 1.11** $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ is a field, where $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $\bar{0}$ is the set of even integers and $\bar{1}$ is the set of odd integers. It follows the additions and multiplications below:

$$
\begin{array}{c|cc} + & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{1} & \bar{0} \end{array} \qquad \begin{array}{c|cc} \times & \bar{0} & \bar{1} \\ \hline \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} \end{array} \tag{1.3}
$$

■

1.3 Morphisms

> **Definition 1.3.1 — Morphisms.** A *morphism* is a structure-preserving map between two algebraic structures (e.g., groups, rings, fields). Formally, let $(A, \cdot_A)$ and $(B, \cdot_B)$ be two algebraic structures. A morphism $f : A \to B$ is a set map / function such that:
>
> $$f(x \cdot_A y) = f(x) \cdot_B f(y) \quad \forall x, y \in A$$

> **Definition 1.3.2 — Monoid Homomorphism.** A *monoid homomorphism* is a morphism between two monoids that preserves the monoid structure. Formally, let $(M_1, \cdot_1)$ and $(M_2, \cdot_2)$ be two monoids with identity elements e_1 and e_2, respectively. A function $f : M_1 \to M_2$ is a monoid homomorphism if:
>
> 1. $f(x \cdot_1 y) = f(x) \cdot_2 f(y) \quad \forall x, y \in M_1$
> 2. $f(e_1) = e_2$

> **Definition 1.3.3 — Group Homomorphism.** A *group homomorphism* is a morphism between two groups that preserves the group structure. Formally, let $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ be two groups with identity elements e_1 and e_2, respectively. A function $f : G_1 \to G_2$ is a group homomorphism if:
>
> 1. $f(x \cdot_1 y) = f(x) \cdot_2 f(y) \quad \forall x, y \in G_1$
> 2. $f(e_1) = e_2$
> 3. $f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G_1$

Proposition 1.3.1 The second and third properties of a group homomorphism are consequences of the first property.

Proof. Let $f : G_1 \to G_2$ be a group homomorphism satisfying the first property. We will show that the second and third properties follow from it.

Second Property: To show that $f(e_1) = e_2$, we use the fact that e_1 is the identity element in G_1. For any element $x \in G_1$, we have:

$$f(x) = f(x \cdot_1 e_1) = f(x) \cdot_2 f(e_1)$$

The equation above holds for all $x \in G_1$. So for any $f(x) \in G_2$, this implies that $f(e_1)$ must be the identity element in G_2, i.e., $f(e_1) = e_2$.

Third Property: To show that $f(x^{-1}) = (f(x))^{-1}$ for all $x \in G_1$, we use the fact that x^{-1} is the inverse of x in G_1. We have:

$$e_2 = f(e_1) = f(x \cdot_1 x^{-1}) = f(x) \cdot_2 f(x^{-1})$$

This shows that $f(x^{-1})$ is the inverse of $f(x)$ in G_2, i.e., $f(x^{-1}) = (f(x))^{-1}$.

Therefore, both the second and third properties of a group homomorphism are indeed consequences of the first property. ∎

R For monoid homomorphisms, the second property cannot be derived from the first property. Consider the identity element e_1 in M_1. If we apply the first property, we get $f(e_1 \cdot_1 e_1) = f(e_1) \cdot_2 f(e_1)$. This simplifies to $f(e_1) = f(e_1) \cdot_2 f(e_1)$, which does not necessarily imply that $f(e_1)$ is the identity element in M_2, i.e., $f(e_1) \neq e_2$, but $f(e_1)$ is the idempotent element in M_2. Therefore, the second property must be explicitly stated for monoid homomorphisms.

However in the case of group homomorphisms, the existence of inverses ensures that there is only one element that can be idempotent under the group operation, which is the identity element. Thus, for group homomorphisms, the second property can be derived from the first property.

Definition 1.3.4 — Ring Homomorphism. A *ring homomorphism* is a morphism between two rings that preserves both the additive and multiplicative structures. Formally, let $(R_1, +_1, \cdot_1)$ and $(R_2, +_2, \cdot_2)$ be two rings with identity elements 0_1, 1_1 and 0_2, 1_2, respectively. A function $f : R_1 \to R_2$ is a ring homomorphism if:

1. $f(x +_1 y) = f(x) +_2 f(y) \quad \forall x, y \in R_1$
2. $f(x \cdot_1 y) = f(x) \cdot_2 f(y) \quad \forall x, y \in R_1$
3. $f(1_1) = 1_2$

Definition 1.3.5 — Endomorphism. An *endomorphism* is a morphism from an algebraic structure to itself. Formally, let $(A, \cdot)$ be an algebraic structure. An endomorphism $f : A \to A$ is a set map such that:

$$f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in A$$

Definition 1.3.6 — Hom-set. The set of all morphisms from an algebraic structure A to another algebraic structure B is called the *hom-set*, denoted by $\text{Hom}(A, B)$.

Definition 1.3.7 — Endomorphism Ring. The set of all endomorphisms of an abelian group $(A, +)$, denoted by $\text{End}(A)$, forms a (non-commutative) ring under pointwise addition and composition of set maps. The addition and multiplication operations are defined as follows:

$$+ : \text{End}(A) \times \text{End}(A) \to \text{End}(A)$$
$$(f, g) \mapsto (f + g : x \mapsto f(x) + g(x)) \qquad f + g : A \to A$$

$$\circ : \text{End}(A) \times \text{End}(A) \to \text{End}(A)$$
$$(f, g) \mapsto (f \circ g : x \mapsto f(g(x))) \qquad f \circ g : A \to A$$

The identity element for addition is the zero endomorphism, which maps every element to the identity element of the group.

$$0 : A \to A$$
$$x \mapsto 0$$

The identity element for multiplication is the identity endomorphism, which maps every element to itself.

$$1 : A \to A$$
$$x \mapsto x$$

Note that all endomorphisms in $\text{End}(A)$ are group homomorphisms and $\text{End}(A) = \text{Hom}(A, A)$.

1.4 Vector Spaces

Definition 1.4.1 — Linear Structure. A *linear structure* over a field F on a set V is a pair $(+, \cdot)$ where $(V, +)$ is an abelian group with a ring homomorphism $F \to \text{End}(V)$, where $\text{End}(V)$ is the endomorphism ring of the abelian group $(V, +)$.

$$\cdot : F \to \text{End}(V)$$
$$\alpha \mapsto (\alpha \cdot : \vec{x} \mapsto \alpha \vec{x}) \qquad \alpha \cdot : V \to V$$

The ring homomorphism is a (ring) action of the field F on the abelian group $(V, +)$, called *scalar multiplication*. The ring action can be written as a binary operation:

$$\cdot : F \times V \to V$$
$$(\alpha, \vec{x}) \mapsto \alpha \vec{x}$$

Definition 1.4.2 — Linear Spaces / Vector Spaces. A linear space / vector space is a set with a linear structure over a field on the set.

Corollary 1.4.1 — Linear Spaces. A linear space over a field F is a set V equipped with two operations: vector addition $+ : V \times V \to V$ and scalar multiplication $\cdot : F \times V \to V$, satisfying the following axioms for all $\vec{u}, \vec{v}, \vec{w} \in V$ and $\alpha, \beta \in F$:

Axiom	Statement
1. Associativity of addition	$(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$
2. Existence of additive identity	$\exists \vec{0} \in V$ such that $\forall \vec{u} \in V, \vec{u} + \vec{0} = \vec{u}$
3. Existence of additive inverses	$\forall \vec{u} \in V, \exists -\vec{u} \in V$ such that $\vec{u} + (-\vec{u}) = \vec{0}$
4. Commutativity of addition	$\vec{u} + \vec{v} = \vec{v} + \vec{u}$
5. Distributivity of scalar multiplication with respect to vector addition	$\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$
6. Distributivity of scalar multiplication with respect to field addition	$(\alpha + \beta) \cdot = \alpha \cdot + \beta \cdot$
7. Compatibility of scalar multiplication with field multiplication	$(\alpha\beta) \cdot = (\alpha \cdot) \circ (\beta \cdot)$
8. Identity element of scalar multiplication	$F \ni 1 = (1 \cdot : x \mapsto x) \in \text{End}(V)$

R Note that the first four axioms ensure that $(V, +)$ is an abelian group, while the fifth axiom describes the endomorphism structure and the last three axioms describe the ring homomorphism.

■ **Example 1.12** F is a linear space over itself with the usual addition and multiplication operations.

$$\cdot : F \times F \to F$$
$$(\alpha, \beta) \mapsto \alpha\beta$$

The first F is the field acting on the second F, which is the abelian group.   ■

■ **Example 1.13** Let X be a set and F be a field. (f is a set map)

$$F[[X]] = \text{Map}(X, F) \stackrel{\text{def}}{=\!=} \text{the set of all } F\text{-valued functions on } X$$
$$= \{f : X \to F\}$$

$F[[X]]$ is a linear space over F with the following operations defined pointwisely:

$$+ : F[[X]] \times F[[X]] \to F[[X]]$$
$$(f, g) \mapsto (f + g : x \mapsto f(x) + g(x)) \qquad f + g : X \to F$$

$$\cdot : F \times F[[X]] \to F[[X]]$$
$$(\alpha, f) \mapsto (\alpha f : x \mapsto \alpha f(x)) \qquad \alpha f : X \to F$$

■

■ **Example 1.14** Let X be a set and F be a field.

$$F[X] = \text{Map}_{\text{fin}}(X, F) \stackrel{\text{def}}{=\!=} \text{the set of all finitely supported } F\text{-valued functions on } X$$
$$= \{f : X \to F \mid f \text{ is finitely supported}\}$$

$F[X]$ is a linear space over F as $F[X] \subseteq F[[X]]$ and the operations are defined pointwisely as in the previous example.

$f : X \to F$ is finitely supported if the set $\{x \in X \mid f(x) \neq 0\}$ is finite or $f(x) \neq 0$ for only finitely many $x \in X$.   ■

■ **Example 1.15** Let t be a formal variable. Then $F[[t]] \stackrel{\text{def}}{=\!=} F[[\{1, t, t^2, \cdots\}]] = \sum_{n=0}^{\infty} a_n t^n$ is the set of all formal power series in t with coefficients in F and $F[t] \stackrel{\text{def}}{=\!=} F[\{1, t, t^2, \cdots\}] = \sum_{n=0}^{N} a_n t^n$ is the set of all polynomials in t with coefficients in F. Both $F[[t]]$ and $F[t]$ are linear spaces over F. ■

■ **Example 1.16** Let n be a positive integer and F be a field. Then

$$F^n \stackrel{\text{def}}{=\!=} \left\{ \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \,\middle|\, c_i \in F \right\}$$

is the set of all *column matrices* with n entries in F. Elements in F^n are written as $\vec{x}$ and are called *column vectors*. F^n is a linear space over F with the following operations defined entrywisely:

$$+ : F^n \times F^n \to F^n$$
$$(\vec{a}, \vec{b}) \mapsto \vec{a} + \vec{b} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

$$\cdot : F \times F^n \to F^n$$
$$(\alpha, \vec{a}) \mapsto \alpha \vec{a} = \begin{bmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{bmatrix}$$

F^n is a linear space over F automatically as F is a linear space over itself.   ■

2. Linear Maps and Matrices

2.1 Linear Maps

Definition 2.1.1 — Linear Maps. Let V and W be two linear spaces over a field F. A linear map is a set map $f : V \to W$ such that for all $\vec{u}, \vec{v} \in V$ and $\alpha \in F$, the following holds:

$$f(\vec{u} + \vec{v}) = f(\vec{u}) + f(\vec{v})$$
$$f(\alpha \vec{u}) = \alpha f(\vec{u})$$

The set of all linear maps from V to W is denoted by $\mathscr{L}(V, W) = \text{Hom}(V, W)$.

Definition 2.1.2 — Linear Combinations. Let V be a linear space over a field F. A *linear combination* of vectors $\vec{v_1}, \vec{v_2}, \cdots, \vec{v_n} \in V$ is a vector of the form:

$$\alpha_1 \vec{v_1} + \alpha_2 \vec{v_2} + \cdots + \alpha_n \vec{v_n}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ are scalars.

Corollary 2.1.1 — Linear Maps and Linear Combinations. A set map $f : V \to W$ between two linear spaces over a field F is a linear map if and only if f respects linear combinations, i.e., for all $\vec{v_1}, \vec{v_2} \in V$ and all scalars $\alpha_1, \alpha_2 \in F$, the following holds:

$$f(\alpha_1 \vec{v_1} + \alpha_2 \vec{v_2}) = \alpha_1 f(\vec{v_1}) + \alpha_2 f(\vec{v_2})$$

■ **Example 2.1** Let A be an $m \times n$ matrix with entries in a field F. The map $T : F^n \to F^m$ defined by

$$T\vec{x} = T(\vec{x}) = A\vec{x}$$

where the multiplication on the right-hand side is the usual matrix multiplication, is a linear map over F. ■

Proposition 2.1.2 A linear map $T : F^n \to F^m$ is a matrix multiplication by a unique $m \times n$ matrix

A with entries in F. The matrix A is called the *standard matrix* of the linear map T.

$$\{\text{Linear maps over } F\} \equiv \{m \times n \text{ matrices over } F\}$$
$$A \cdot : \vec{x} \mapsto A\vec{x} \hookleftarrow A$$
$$T \mapsto A = \begin{bmatrix} T\vec{e}_1 & T\vec{e}_2 & \cdots & T\vec{e}_n \end{bmatrix}$$

where the $\equiv$ sign means they are natural identifications and $\vec{e}_i \in F^n$ is the i-th standard basis vector, i.e., the column matrix with 1 in the i-th row and 0 elsewhere.

Proof. Consider a column matrix $\vec{x} \in F^n$ with entries $x_1, x_2, \cdots, x_n \in F$. Then $\vec{x}$ can be expressed as a linear combination of the standard basis vectors $\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_n$:

$$\vec{x} = x_1\vec{e}_1 + x_2\vec{e}_2 + \cdots + x_n\vec{e}_n = \sum_{i=1}^{n} x_i\vec{e}_i$$

Since T is a linear map, it respects linear combinations. Therefore, we have:

$$T\vec{x} = T\left(\sum_{i=1}^{n} x_i\vec{e}_i\right) = \sum_{i=1}^{n} x_i T(\vec{e}_i) = \sum_{i=1}^{n} x_i\vec{a}_i = A\vec{x}$$

where $\vec{a}_i = T(\vec{e}_i)$ is the i-th column of the matrix $A = \begin{bmatrix} T\vec{e}_1 & T\vec{e}_2 & \cdots & T\vec{e}_n \end{bmatrix}$. Thus, we have $T\vec{x} = A\vec{x}$ for all $\vec{x} \in F^n$. This shows that T can be represented as a matrix multiplication by the matrix A. $\blacksquare$

R There is a simpler way to write $\sum_{i=1}^{n} x_i\vec{e}_i$: The Eienstein summation convention. When an index variable appears twice in a single term and is not otherwise defined, it implies summation of that term over all the values of the index. Therefore, we can write:

$$\vec{x} = x_i\vec{e}_i$$

where i is summed from 1 to n.

Definition 2.1.3 — Homogeneous Linear Functions. A linear map $f : F^n \to F$ is called a *homogeneous linear function* or a *linear functional* if it satisfies the property:

$$f(\alpha\vec{x}) = \alpha f(\vec{x}) \quad \text{for all } \alpha \in F \text{ and } \vec{x} \in F^n.$$

Corollary 2.1.3 — Standard Matrix of a Linear Map. The standard matrix of a linear map $T : F^n \to F^m$ can be written as:

$$A = \begin{bmatrix} f_1(\vec{e}_1) & f_1(\vec{e}_2) & \cdots & f_1(\vec{e}_n) \\ f_2(\vec{e}_1) & f_2(\vec{e}_2) & \cdots & f_2(\vec{e}_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_m(\vec{e}_1) & f_m(\vec{e}_2) & \cdots & f_m(\vec{e}_n) \end{bmatrix}$$

where $f_i : F^n \to F$ is the i-th component function of T, i.e., $T\vec{x} = \begin{bmatrix} f_1(\vec{x}) \\ f_2(\vec{x}) \\ \vdots \\ f_m(\vec{x}) \end{bmatrix}$ for all $\vec{x} \in F^n$.

  R Each component function f_i is a homogeneous linear function, and the standard matrix A is constructed by evaluating these functions at the standard basis vectors $\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_n$ of F^n.

■ **Example 2.2** Let $D : F[t] \to F[t]$ be the differentiation operator defined by:

$$D\left(\sum_{n=0}^{N} a_n t^n\right) = \sum_{n=1}^{N} n a_n t^{n-1}$$

for all polynomials $\sum_{n=0}^{N} a_n t^n \in F[t]$. The differentiation operator D is a linear map over F. The standard matrix of D with respect to the standard basis $\{1, t, t^2, \cdots, t^N\}$ of $F[t]$ is given by:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & N \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

■

2.2 Injective and Surjective Linear Maps and Linear Equivalences

Definition 2.2.1 — Injective Linear Maps. A linear map $f : V \to W$ between two linear spaces over a field F is said to be *injective* (or one-to-one) if for all $\vec{u}, \vec{v} \in V$, the following holds:

$$f(\vec{u}) = f(\vec{v}) \implies \vec{u} = \vec{v}$$

Equivalently, f is injective if the only vector in V that maps to the zero vector in W is the zero vector itself:

$$f(\vec{u}) = 0 \implies \vec{u} = 0$$

Definition 2.2.2 — Surjective Linear Maps. A linear map $f : V \to W$ is said to be *surjective* (or onto) if for every $\vec{w} \in W$, there exists at least one $\vec{v} \in V$ such that:

$$f(\vec{v}) = \vec{w}$$

Definition 2.2.3 — Linear Equivalences / Isomorphisms. A linear map $T : V \to W$ is called a *linear equivalence*, *isomorphism* or *invertible linear map* if T has a unique two-sided inverse S, denoted by T^{-1}, i.e., there exists a linear map $S : W \to V$ such that:

$$T S = e_W \quad \text{and} \quad S T = e_V$$

where $e_V : V \to V$ and $e_W : W \to W$ are the identity maps on V and W, respectively. In this case, we say that the linear spaces V and W are *isomorphic*, denoted by $V \cong W$.

Corollary 2.2.1 — Linear Equivalences. A linear map $T : V \to W$ is a linear equivalence if and only if T is both injective and surjective, i.e., bijective / one-to-one correspondence.

Proof. ($\Rightarrow$) Assume $T : V \to W$ is a linear equivalence. By definition, there exists a linear map $S : W \to V$ such that $T S = e_W$ and $S T = e_V$.

To show that T is injective, suppose $T(\vec{u}) = T(\vec{v})$ for some $\vec{u}, \vec{v} \in V$. Applying S to both sides, we have:

$$S(T(\vec{u})) = S(T(\vec{v})) \implies (ST)(\vec{u}) = (ST)(\vec{v}) \implies e_V(\vec{u}) = e_V(\vec{v}) \implies \vec{u} = \vec{v}$$

Thus, T is injective.

To show that T is surjective, let $\vec{w} \in W$. Since $T S = e_W$, we have:

$$T(S(\vec{w})) = e_W(\vec{w}) = \vec{w}$$

This shows that for every $\vec{w} \in W$, there exists a $\vec{v} = S(\vec{w}) \in V$ such that $T(\vec{v}) = \vec{w}$. Thus, T is surjective.

($\Leftarrow$) Now assume that $T : V \to W$ is both injective and surjective. We need to show that there exists a linear map $S : W \to V$ such that $T S = e_W$ and $S T = e_V$.

Since T is surjective, for each $\vec{w} \in W$, there exists at least one $\vec{v} \in V$ such that $T(\vec{v}) = \vec{w}$. Define the map $S : W \to V$ by choosing one such preimage for each $\vec{w}$:

$$S(\vec{w}) = \text{a chosen } \vec{v} \text{ such that } T(\vec{v}) = \vec{w}$$

To show that S is well-defined, we need to ensure that if $T(\vec{v_1}) = T(\vec{v_2})$, then $\vec{v_1} = \vec{v_2}$. This follows from the injectivity of T. Now we verify that $T S = e_W$:

$$(TS)(\vec{w}) = T(S(\vec{w})) = \vec{w}$$

for all $\vec{w} \in W$. Thus, $TS = e_W$. Next, we verify that $ST = e_V$:

$$(ST)(\vec{v}) = S(T(\vec{v})) = \vec{v}$$

for all $\vec{v} \in V$. Thus, $ST = e_V$. Therefore, T has a two-sided inverse S, and hence T is a linear equivalence. ∎

Proposition 2.2.2 Let $T : V \to W$ be a linear map between two linear spaces over a field F and $T^{-1} : W \to V$ be the set-theoretical inverse of T. Then T^{-1} is also a linear map.

Proof. Since T is a linear equivalence, it is bijective, and thus has a well-defined set-theoretical inverse $T^{-1} : W \to V$. We need to show that T^{-1} is a linear map, i.e., it respects vector addition and scalar multiplication.

Let $\vec{w}_1, \vec{w}_2 \in W$ and $\alpha \in F$. We will show that:

$$T^{-1}(\vec{w}_1 + \vec{w}_2) = T^{-1}(\vec{w}_1) + T^{-1}(\vec{w}_2)$$

and

$$T^{-1}(\alpha \vec{w}_1) = \alpha T^{-1}(\vec{w}_1)$$

Since T is surjective, there exist $\vec{v}_1, \vec{v}_2 \in V$ such that $T(\vec{v}_1) = \vec{w}_1$ and $T(\vec{v}_2) = \vec{w}_2$. Then we have:

$$T^{-1}(\vec{w}_1 + \vec{w}_2) = T^{-1}(T(\vec{v}_1) + T(\vec{v}_2)) = T^{-1}(T(\vec{v}_1 + \vec{v}_2)) = \vec{v}_1 + \vec{v}_2$$

On the other hand, we also have:

$$T^{-1}(\vec{w}_1) + T^{-1}(\vec{w}_2) = \vec{v}_1 + \vec{v}_2$$

Thus, we conclude that:

$$T^{-1}(\vec{w}_1 + \vec{w}_2) = T^{-1}(\vec{w}_1) + T^{-1}(\vec{w}_2)$$

Next, we show that T^{-1} respects scalar multiplication. For any scalar $\alpha \in F$, we have:

$$T^{-1}(\alpha \vec{w}_1) = T^{-1}(\alpha T(\vec{v}_1)) = T^{-1}(T(\alpha \vec{v}_1)) = \alpha \vec{v}_1$$

On the other hand, we also have:

$$\alpha T^{-1}(\vec{w}_1) = \alpha \vec{v}_1$$

Thus, we conclude that:

$$T^{-1}(\alpha \vec{w}_1) = \alpha T^{-1}(\vec{w}_1)$$

Therefore, T^{-1} respects both vector addition and scalar multiplication, and hence T^{-1} is a linear map. ∎

Proposition 2.2.3 Let X be a set and W be a linear space over a field F. Then the set of all set maps from X to W, denoted by $\mathrm{Map}(X, W)$, is a linear space over F with the following operations defined pointwise:

$$+ : \mathrm{Map}(X, W) \times \mathrm{Map}(X, W) \to \mathrm{Map}(X, W)$$
$$(f, g) \mapsto (f + g : x \mapsto f(x) + g(x)) \qquad f + g : X \to W$$

$$\cdot : F \times \mathrm{Map}(X, W) \to \mathrm{Map}(X, W)$$
$$(\alpha, f) \mapsto (\alpha f : x \mapsto \alpha f(x)) \qquad \alpha f : X \to W$$

Proposition 2.2.4 Let V and W be two linear spaces over a field F. Then $\operatorname{Hom}(V,W)$ is a linear space over F with the following operations defined pointwisely:

$$+ : \operatorname{Hom}(V,W) \times \operatorname{Hom}(V,W) \to \operatorname{Hom}(V,W)$$
$$(f,g) \mapsto (f+g : \vec{v} \mapsto f(\vec{v}) + g(\vec{v})) \qquad f+g : V \to W$$

$$\cdot : F \times \operatorname{Hom}(V,W) \to \operatorname{Hom}(V,W)$$
$$(\alpha, f) \mapsto (\alpha f : \vec{v} \mapsto \alpha f(\vec{v})) \qquad \alpha f : V \to W$$

Proof. Note that $\operatorname{Hom}(V,W) \subseteq \operatorname{Map}(V,W)$. We need to show that the operations defined above are closed in $\operatorname{Hom}(V,W)$, i.e., for all $f,g \in \operatorname{Hom}(V,W)$ and $\alpha \in F$, $f+g \in \operatorname{Hom}(V,W)$ and $\alpha f \in \operatorname{Hom}(V,W)$ or equivalently, f respects linear combinations.

Let $\vec{u}, \vec{v} \in V$ and $\alpha, \beta \in F$. Since $f,g \in \operatorname{Hom}(V,W)$, we have:

$$(f+g)(\alpha\vec{u} + \beta\vec{v}) \overset{\text{def}}{=\!=} f(\alpha\vec{u} + \beta\vec{v}) + g(\alpha\vec{u} + \beta\vec{v})$$
$$\overset{\text{lin}}{=\!=} \alpha f(\vec{u}) + \beta f(\vec{v}) + \alpha g(\vec{u}) + \beta g(\vec{v})$$
$$= \alpha(f(\vec{u}) + g(\vec{u})) + \beta(f(\vec{v}) + g(\vec{v}))$$
$$\overset{\text{def}}{=\!=} \alpha(f+g)(\vec{u}) + \beta(f+g)(\vec{v})$$

where "lin" denotes the linearity of f and g. Thus, $f+g \in \operatorname{Hom}(V,W)$ and $\alpha f \in \operatorname{Hom}(V,W)$. ∎

R   Note that $\operatorname{End}(V) = \operatorname{Hom}(V,V)$ is a linear space over F and also a ring with the addition and multiplication operations defined in the previous section. The addition operation is commutative, but the multiplication operation is not necessarily commutative.

Then we can say that

$$\operatorname{Map}(F^n, F^m) \supseteq \operatorname{Hom}(F^n, F^m) \cong M_{m \times n}(F) := \{\text{the set of all } m \times n \text{ matrices over } F\}$$

Definition 2.2.4 — Characteristic of a Field. The *characteristic* of a field F is the smallest positive integer n such that:
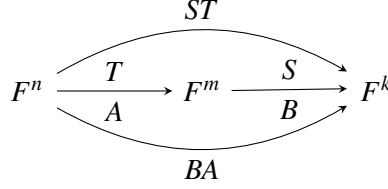
$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

If no such positive integer exists, the characteristic of F is defined to be 0.

■ **Example 2.3** The differentiation operator $D : F[t] \to F[t]$ is not an injective linear map as $D(1) = 0 = D(2)$ but is a surjective linear map if F is a field of characteristic 0. ■

2.3   Matrix Multiplications and Compositions of Linear Maps

We consider two linear maps $T : F^n \to F^m$ and $S : F^m \to F^k$ with standard matrices A and B, respectively. We want to find the standard matrix of the composition $ST : F^n \to F^k$.

$$
\begin{array}{ccccc}
& & ST & & \\
& T & & S & \\
F^n & \xrightarrow{\quad\quad} & F^m & \xrightarrow{\quad\quad} & F^k \\
& A & & B & \\
& & BA & &
\end{array}
$$

Proposition 2.3.1 The standard matrix of the composition $ST : F^n \to F^k$ is the matrix multiplication BA, i.e., for all $\vec{x} \in F^n$,

$$(ST)\vec{x} = B(A\vec{x}) = (BA)\vec{x}$$

Proof. Let $\vec{x} \in F^n$ be a column matrix with entries $x_1, x_2, \cdots, x_n \in F$. Then $\vec{x}$ can be expressed as a linear combination of the standard basis vectors $\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_n$:

$$\vec{x} = x_1\vec{e}_1 + x_2\vec{e}_2 + \cdots + x_n\vec{e}_n = \sum_{i=1}^{n} x_i\vec{e}_i$$

Consider the j-th column of BA, it is given by:

$$(ST)\vec{e}_j = S(T(\vec{e}_j)) = S(\vec{a}_j) = B\vec{a}_j = (BA)\vec{e}_j$$

for all $j = 1, 2, \ldots, n$. This shows that the standard matrix of the composition ST is indeed the matrix multiplication BA.   ■

(R) Note that B is a $k \times m$ matrix and A is an $m \times n$ matrix, so the matrix multiplication BA is defined and results in a $k \times n$ matrix.

(R) The matrix multiplication BA can be computed as follows:

$$BA = B[\vec{a}_1 \ \vec{a}_2 \ \cdots \ \vec{a}_n] = [B\vec{a}_1 \ B\vec{a}_2 \ \cdots \ B\vec{a}_n]$$

where $\vec{a}_i = T(\vec{e}_i)$ is the i-th column of the matrix A. Also,

$$B\vec{x} = x_1\vec{b}_1 + x_2\vec{b}_2 + \cdots + x_n\vec{b}_n = \sum_{i=1}^{n} x_i\vec{b}_i$$

where $\vec{b}_i = B\vec{a}_i$ is the i-th column of the matrix B. Note that B is a $k \times m$ matrix, and $\vec{x} \in F^m$. Thus, the matrix multiplication $B\vec{x}$ is defined and results in a column matrix in F^k.

2.4 Elementary Row Operations

> **Definition 2.4.1 — Elementary Row Operations.** Let A be an $m \times n$ matrix over a field F. An *elementary row operation* on A is one of the following operations:
> 1. Interchange two rows of A: $R_i \leftrightarrow R_j$.
> 2. Multiply a row of A by a nonzero scalar in F: $R_i \to \alpha R_i$ where $\alpha \in F \setminus \{0\}$.
> 3. Add a scalar multiple of one row of A to another row of A: $R_i \to R_i + \alpha R_j$ where $\alpha \in F$ and $i \neq j$.
>
> Each elementary row operation can be represented by *left multiplication* of A by an appropriate $m \times m$ matrix over F. Note that all of them are invertible linear maps from $F^{m \times n}$ to $F^{m \times n}$.

For easier notations, we introduce the idea of matrix units, which is similar to the standard basis vectors $\vec{e}_i$.

> **Definition 2.4.2 — Matrix Units.** Let m and n be two positive integers and F be a field. The *matrix unit E_{ij}* is the $m \times n$ matrix over F with 1 in the (i, j)-th position and 0 elsewhere, i.e.,
>
> $$(E_{ij})_{kl} = \begin{cases} 1 & \text{if } (k,l) = (i,j) \\ 0 & \text{otherwise} \end{cases}$$
>
> for all $1 \leq k \leq m$ and $1 \leq l \leq n$.
> It can also be defined as $E_{ij} = \vec{e}_i \hat{e}_j \in M_{m \times n}(F)$ where $\vec{e}_i \in F^m$ and $\vec{e}_j^{\,T} = \hat{e}_j \in F^n$ are the i-th and j-th standard basis vectors, respectively. The $\hat{e}_j$ is the row matrix with 1 in the j-th column and 0 anywhere else.

> **R**   Note that for any $m \times n$ matrix A over a field F, we have:
>
> $$A\vec{e}_j = \text{the } j\text{-th column of } A \in F^n$$
> $$\hat{e}_i A = \text{the } i\text{-th row of } A \in (F^m)^*$$
>
> where $(F^m)^*$ is the set of all row matrices with n entries in F. $\hat{e}_i$ is an element in $(F^m)^*$ for any $1 \leq i \leq m$. Then we have:
>
> $$a_{ij} = \hat{e}_i A \vec{e}_j = \text{the } (i,j)\text{-th entry of } A$$

We can write the $E_{i,j}$ as:

$$E_{i,j} = \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \leftarrow \text{the } j\text{-row} \\ \\ \\ \\ \end{matrix}$$

the i-column (pointing to the middle column)

Then we consider the row operations by using the matrix units.

Proposition 2.4.1 The row operation $R_i \leftrightarrow R_j$ is a linear map where the standard matrix is $A_{R_i \leftrightarrow R_j} = I - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.

Proof. The linear map $T : F^n \to F^n$ is defined pointwisely. We can say the map is:

$$\vec{e}_k \mapsto \begin{cases} \vec{e}_j & \text{if } k = i \\ \vec{e}_i & \text{if } k = j \\ \vec{e}_k & \text{if } k \neq i, j \end{cases}$$

Then the standard matrix of T is:

$$A_{R_i \leftrightarrow R_j} = [\vec{e}_1 \ \cdots \ \vec{e}_j \ \cdots \ \vec{e}_i \ \cdots \ \vec{e}_n] = I - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$$

where I is the $n \times n$ identity matrix. ∎

Proposition 2.4.2 The row operation $R_i \to \alpha R_i$ where $\alpha \in F^x := F \setminus \{0\}$ is a linear map where the standard matrix is $A_{R_i \to \alpha R_i} = I + (\alpha - 1)E_{i,i}$.

Proof. The linear map $T : F^n \to F^n$ is defined pointwisely. We can say the map is:

$$\vec{e}_k \mapsto \begin{cases} \alpha \vec{e}_i & \text{if } k = i \\ \vec{e}_k & \text{if } k \neq i \end{cases}$$

Then the standard matrix of T is:

$$A_{R_i \to \alpha R_i} = [\vec{e}_1 \ \cdots \ \alpha \vec{e}_i \ \cdots \ \vec{e}_n] = I + (\alpha - 1)E_{i,i}$$

where I is the $n \times n$ identity matrix. ∎

Proposition 2.4.3 The row operation $R_i \to R_i + \alpha R_j$ where $\alpha \in F$ and $i \neq j$ is a linear map where the standard matrix is $A_{R_i \to R_i + \alpha R_j} = I + \alpha E_{i,j}$.

Proof. The linear map $T : F^n \to F^n$ is defined pointwisely. We can say the map is:

$$\vec{e}_k \mapsto \begin{cases} \vec{e}_i + \alpha \vec{e}_j & \text{if } k = i \\ \vec{e}_k & \text{if } k \neq i \end{cases}$$

Then the standard matrix of T is:

$$A_{R_i \to R_i + \alpha R_j} = [\vec{e}_1 \ \cdots \ (\vec{e}_i + \alpha \vec{e}_j) \ \cdots \ \vec{e}_n] = I + \alpha E_{i,j}$$

where I is the $n \times n$ identity matrix. ∎

2.5 Dimensions of Vector Spaces

Definition 2.5.1 — Finite Dimensional Vector Spaces. A linear space V over a field F is said to be *finite dimensional* if there exists a linear equivalence $T : V \to F^n$ for some positive integer n. In this case, we say that the dimension of V is n, denoted $\dim_F V = n$ or simply $\dim V = n$.

Definition 2.5.2 — Infinite Dimensional Vector Spaces. A linear space V over a field F is said to be *infinite dimensional* if V is not finite dimensional.

We have to proof if the dimension of a finite dimensional vector space is well-defined.

Proposition 2.5.1 If there exists two linear equivalences $T : V \to F^m$ and $S : V \to F^n$, then $n = m$.

Proof. Since S is linear equivalence, it has a unique two-sided inverses $S^{-1} : F^n \to V$. Consider the composition of this map:

$$TS^{-1} : F^n \to F^m$$

Since TS^{-1} is compositions of linear equivalences, it is also a linear equivalence. Mutantis mutandis, for the opposite direction.

Now, we know that a linear equivalence between two finite-dimensional vector spaces. Then we have $\dim F^n = \dim F^m$ or $n = m$. Thus, the dimension of a finite dimensional vector space is well-defined. ∎

Graphically, we have the following commutative diagram:

$$
\begin{array}{ccc}
 & V & \\
{}^{S}\swarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\searrow{}^{T} \\
F^n & \xrightarrow[\cong]{TS^{-1}} & F^m
\end{array}
$$

R In drawing commutative diagram, we can use $\hookrightarrow$ to denote an injective linear map, $\twoheadrightarrow$ to denote a surjective linear map, and $\cong$ to denote a linear equivalence.

2.6 Elementary Column Operations, Canonical Form and Rank

> **Definition 2.6.1 — Elementary Column Operations.** Let A be an $m \times n$ matrix over a field F. An *elementary column operation* on A is one of the following operations:
> 1. Interchange two columns of A: $C_i \leftrightarrow C_j$.
> 2. Multiply a column of A by a nonzero scalar in F: $C_i \to \alpha C_i$ where $\alpha \in F \setminus \{0\}$.
> 3. Add a scalar multiple of one column of A to another column of A: $C_i \to C_i + \alpha C_j$ where $\alpha \in F$ and $i \neq j$.
>
> Each elementary column operation can be represented by *right multiplication* of A by an appropriate $n \times n$ matrix over F. Note that all of them are invertible linear maps from $F^{m \times n}$ to $F^{m \times n}$.

Proposition 2.6.1 Any $m \times n$ matrix A can be transformed into a matrix of the form $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ by a finite sequence of elementary row and column operations on A, where r is the rank of A.

$$
\begin{array}{ccc}
F^n & \xrightarrow{\;\;A\;\;} & F^m \\
\Big\downarrow{\scriptstyle Q}\;\cong & & \cong\;\Big\downarrow{\scriptstyle P} \\
F^n & \xrightarrow[\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}]{} & F^m
\end{array}
$$

Note that P is the product of a finite sequence of elementary row operation matrices and Q is the product of a finite sequence of elementary column operation matrices. Both P and Q are invertible matrices. Thus, we have:

$$
\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = PAQ^{-1}
$$

> **Definition 2.6.2 — Canonical Form of a Matrix.** The matrix $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ obtained from an $m \times n$ matrix A by a finite sequence of elementary row and column operations on A is called the *canonical form* of A.

> (R) The canonical form of a matrix defined above is also called the *Smith Normal Form* or *Normal Form* of a matrix.

> **Definition 2.6.3 — Rank of a Matrix.** The *rank* of an $m \times n$ matrix A over a field F, denoted by rank(A), is the number of leading 1's in the matrix $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ obtained from A by a finite sequence of elementary row and column operations on A.

> (R) The value r is uniquely determined by A.

Proposition 2.6.2 Let A be an $n \times n$ matrix over a field F. Then the following statements are equivalent:

$$
A \text{ is invertible} \iff m\left\{\underbrace{\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}}_{n} \text{ is invertible} \iff \text{rank}(A) = m = n \iff \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = I_n\right.
$$

Proposition 2.6.3 Let A be an $m \times n$ matrix over a field F. Then the following statements are equivalent:

$$\text{rank}(A) = n \iff A \text{ has a right inverse} \iff A \text{ is injective} \iff \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} I_n \\ 0 \end{bmatrix}$$

Proposition 2.6.4 Let A be an $m \times n$ matrix over a field F. Then the following statements are equivalent:

$$\text{rank}(A) = m \iff A \text{ has a left inverse} \iff A \text{ is surjective} \iff \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} I_m & 0 \end{bmatrix}$$

Proposition 2.6.5 For every $\vec{b}$, $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \vec{x} = \vec{b}$ has a unique solution.

Linear Algebra is the study of linear map between two finite dimensional vector spaces.

$$\dim V = n \qquad \dim W = m$$

The bended arrows denote the trivialisation of the vector spaces and the bottom arrow denotes the canonical matrix representation of the linear map T.

2.7 Linearly Independent Sets, Spanning Sets and Bases

Given a linear space V over a field F. We define the order set $S := \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\} \subseteq V$. The order set S forms a linear map $\phi_S : F^n \to V$ defined by:

$$\phi_S(\vec{x}) = \phi_S\left(\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\right) = x_1\vec{v}_1 + x_2\vec{v}_2 + \cdots + x_n\vec{v}_n = \sum_{i=1}^{n} x_i\vec{v}_i$$

Definition 2.7.1 — Linearly Independent Sets. The order set $S := \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\} \subseteq V$ is said to be *linearly independent* if the linear map $\phi_S : F^n \to V$ defined above is injective.

Definition 2.7.2 — Spanning Sets. The order set $S := \{\vec{v}_1, \vec{v}_2, \cdots, \vec{v}_n\} \subseteq V$ is said to be a *spanning set* of V if the linear map $\phi_S : F^n \to V$ defined above is surjective.