1 Chapter

**Defn 1** Field Axioms. A set $F$ with operations $+$ and $\cdot$ and distinguished elements 0 and 1 with $0 \neq 1$ is a **field** if the following properties hold for all $x, y, z \in F$.

**A0:** $x + y \in S$. Closure of addition.

**M0:** $x \cdot y \in S$. Closure of multiplication.

**A1:** $(x + y) + z = x + (y + z)$. Associativity of addition.

**M1:** $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Associativity of multiplication.

**A2:** $x + y = y + x$. Commutativity of addition.

**M2:** $x \cdot y = y \cdot x$. Commutativity of multiplication.

**A3:** $x + 0 = x$. Additive identity.

**M3:** $x \cdot 1 = x$. Multiplicative identity.

**A4:** Given $x$, there is a $w \in S$ such that $x + w = 0$. Additive inverse.

**M4:** Given $x \neq 0$, there is a $w \in S$ such that $x \cdot w = 1$. Multiplicative inverse.

**DL:** $x \cdot (y + z) = x \cdot y + x \cdot z$. Distributive Law.

The operations $+$ and $\cdot$ are called **addition** and **multiplication**. The elements 0 and 1 are the **additive identity element** and the **multiplicative identity element**.

Commonly used in this course: $\mathbb{R}$, $\mathbb{C}$.

Rarely used in this course: $\mathbb{Q}$, $\mathbb{Z}$.

Not a field: $\mathbb{Z}$. 

Defn 2 A vector space $V$ over a field $F$ consists of a set on which two operations, which are called addition and scalar multiplication are defined so that for each pair of elements $x, y$ in $V$, there is a unique element $x + y$ in $V$, and for each element $a$ in $F$ and each element $x$ in $V$, there is a unique element $ax$ in $V$, such that the following conditions hold.

(VS 1) For all $x, y$ in $V$, $x + y = y + x$ commutativity of addition

(VS 2) For all $x, y, z$ in $V$, $(x + y) + z = x + (y + z)$ associativity of addition

(VS 3) There exists an element in $V$ denoted by 0 such that $x + 0 = x$ for each $x$ in $V$.

(VS 4) For each element $x$ in $V$, there exists an element $y$ in $V$ such that $x + y = 0$.

(VS 5) For each $x \in V$, $1x = x$.

(VS 6) For each pair of elements $a, b \in F$ and each element $x \in V$, $(ab)x = a(bx)$.

(VS 7) For each element $a$ in $F$ and each pair of elements $x, y$ in $V$, $a(x + y) = ax + ay$.

(VS 8) For each pair of elements $a, b \in F$, and each element $x \in V$, $(a + b)x = ax + bx$. 
Example 1 Vectors: \( \mathbb{R}^n, \mathbb{C}^n, \) or \( F^n \) for any field \( F \).
Matrices: \( M_{m \times n}(F) \) for any field \( F \).
Function space: \( \mathcal{F}(S, F) \) for nonempty set \( S \) and field \( F \).
Polynomials: \( \mathbf{P}(F) \)

Defn 3 A subset \( W \) of a vector space \( V \) over a field \( F \) is called a subspace of \( V \) if \( W \) is a vector space over \( F \) with the operations of addition and scalar multiplication defined on \( V \).

Theorem 1.3 Let \( V \) be a vector space and \( W \) a subset of \( V \). Then \( W \) is a subspace of \( V \) if and only if the following three conditions hold for the operations defined in \( V \).

1. \( 0 \in W \).
2. \( x + y \in W \) whenever \( x \in W \) and \( y \in W \).
3. \( cx \in W \) whenever \( c \in F \) and \( x \in W \).
Defn 4. Let $V$ be a vector space and $S$ a nonempty subset of $V$. A vector $v$ is called a **linear combination** of vectors of $S$ if there exist a finite number of vectors $u_1, u_2, \ldots, u_n$ in $S$ and scalars $a_1, a_2, \ldots, a_n$ in $F$ such that $v = a_1 u_1 + a_2 u_2 + \cdots + a_n u_n$. We call $a_i$ for all $i \in \{1, \ldots, n\}$ the **coefficients** of the linear combination.

The **span** of $S$, denoted $\text{span}(S)$, is the set of all linear combinations of the vectors of $S$. By convention, $\text{span}(\emptyset) = \{0\}$. Also note that $S \subseteq \text{span}(S)$.

---

**Theorem 1.5**. The span of any subset $S$ of a vector space $V$ is a subspace of $V$. Moreover, any subspace of $V$ that contains $S$ must also contain the span of $S$.

**Proof.** We need to show that $0 \in \text{span}(S)$,

$x, y \in \text{span}(S)$ implies $x + y \in \text{span}(S)$,

and $ax \in \text{span}(S)$ whenever $a \in F$.

First note that $0 \in F$ and $S$ is nonempty so it contains some $x$. We know $0 \cdot x = \emptyset$, and so $0$ is in $\text{span}(S)$.
Now, denote \( x \in \text{span}(S) \) by
\[
x = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n.
\]
and \( y \in \text{span}(S) \) by
\[
y = b_1 u_1 + b_2 u_2 + \cdots + b_m u_m.
\]
Then
\[
x + y = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n + b_1 u_1 + b_2 u_2 + \cdots + b_m u_m.
\]
Some vectors may be repeated in the sum, but by property (VS 8) if \( v_i = u_j = v \), then \( a_i v_i + b_j u_j = a_i v + b_j v = (a_i + b_j) v \) and so \( x + y \in \text{span}(S) \)

\[
ax = a(a_1 v_1 + a_2 v_2 + \cdots + a_n v_n)
\]
By (VS 7), we have
\[
= a \cdot a_1 v_1 + a \cdot a_2 v_2 + \cdots + a \cdot a_n v_n
\]
For each \( i, a \cdot a_i \in F \), by closure of multiplication. Thus, \( ax \in \text{span}(S) \).
Furthermore, let $W$ be a subspace of $V$ and $S \subseteq W$ we wish to prove that $\text{span}(S) \subseteq W$. Let $x \in \text{span}(S)$, then

$x = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, for some vectors $v_1, v_2, \ldots, v_n$ in $S$. But $v_1, v_2, \ldots, v_n$ are also in $W$ since $S \subseteq W$. By closure of scalar multiplication we have for each $i$, $a_iv_i \in W$ and by closure of addition of vectors and induction,

$x = a_1v_1 + a_2v_2 + \cdots + a_nv_n$ is in $W$. 

\[ \square \]

---

**Cor 1** If $S$ is a subspace of $V$, then $\text{span}(S) = S$.

**Proof.** By the previous theorem, with $S$ playing the role of $W$ and using that $S \subseteq S$, we have $\text{span}(S) \subseteq S$. By definition, $S \subseteq \text{span}(S)$. So, $\text{span}(S) = S$. 

\[ \square \]
Defn 5 A set \( S \) generates a vector space \( V \) if \( \text{span}(S) = V \).

Example 2 \( \mathbb{R}^2 = V \) and \( \{(1,0),(0,1)\} = S \).

Defn 6 A subset \( S \) of a vector space \( V \) is called linearly dependent if there exists a finite number of distinct vectors, and scalars, not all zero, such that
\[
a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0.
\]

Also, we say that \( \{v_1, \ldots, v_n\} \) is linearly dependent. If no such set exists, then \( S \) is called linearly independent.

Theorem 1.6 Let \( V \) be a vector space, and let \( S_1 \subseteq S_2 \subseteq V \).
If \( S_1 \) is linearly dependent, then \( S_2 \) is linearly dependent.
Also, if \( S_2 \) is linearly independent, then \( S_1 \) is linearly independent.

Cor 2 Let \( V \) be a vector space, and let \( S_1 \subseteq S_2 \subseteq V \). If \( S_2 \) is linearly independent, then \( S_1 \) is linearly independent.

One of the presentations.
Theorem 1.7 Let $S$ be a linearly independent subset of a vector space $V$, and let $v$ be a vector in $V$ that is not in $S$. Then $S \cup \{v\}$ is linearly dependent if and only if $v \in \text{span}(S)$.

Proof. If $S \cup \{v\}$ is linearly dependent, then there are vectors $u_1, \ldots, u_n$ in $S \cup \{v\}$ such that
\[ a_1u_1 + a_2u_2 + \cdots + a_nu_n = 0 \]
for some nonzero scalars $a_1, \ldots, a_n$. Because $S$ is linearly independent, one of the $u_i$'s, say $u_1$, equals $v$. Thus $a_1v + a_2u_2 + \cdots + a_nu_n = 0$, and so
\[ v = a_1^{-1}(-a_2u_2 - \cdots - a_nu_n) = -(a_1^{-1}a_2)u_2 - \cdots - (a_1^{-1}a_n)u_n. \]
Since $v$ is a linear combination of $u_2, \ldots, u_n$, which are in $S$, we have $v \in \text{span}(S)$.

Conversely, let $v \in \text{span}(S)$. Then there exists vectors $v_1, v_2, \ldots, v_m$ in $S$ and scalars $b_1, b_2, \ldots, b_m$ such that
\[ v = b_1v_1 + \cdots + b_mv_m. \]
Hence
\[ 0 = b_1v_1 + \cdots + b_mv_m + (-1)v. \]
Since $v \neq v$, for $i = 1, 2, \ldots, m$, the coefficient of $v$ in this linear combination is nonzero, and so the set $\{v_1, v_2, \ldots, v_m, v\}$ is linearly dependent. Therefore, $S \cup \{v\}$ is linearly dependent by Theorem 1.6. \hfill \Box
Defn 7 A basis $\beta$ for a vector space $V$ is a linearly independent subset of $V$ that generates $V$. If $\beta$ is a basis for $V$, we also say that the vectors of $\beta$ form a basis for $V$.

Theorem 1.8 Let $V$ be a vector space and $\beta = \{u_1, u_2, \ldots, u_n\}$ be a subset of $V$. Then $\beta$ is a basis for $V$ if and only if each $v \in V$ can be uniquely expressed as a linear combination of vectors of $\beta$, that is, can be expressed in the form

$$v = a_1u_1 + a_2u_2 + \cdots + a_nu_n$$

for unique scalars $a_1, a_2, \ldots, a_n$.

Proof. $(\Leftarrow)$ We know $\beta$ spans $V$ because each vector can be written as linear combination of vectors in $\beta$.

If $\beta$ is linearly dependent, there exists scalars $\{a_1, \ldots, a_n\}$ not all zero such that $0 = a_1u_1 + \cdots + a_nu_n$. But also, $0 = 0u_1 + \cdots + 0u_n$.

by uniqueness, it must be that $a_i = 0$ for each $i$. This is a contradiction, so $\beta$ is linearly independent.
The basis $\beta$ spans $V$, so we have that each vector can be written as a linear combination of vectors in $\beta$. Suppose there are 2 different ways to express $v$:

$$v = a_1u_1 + a_2u_2 + \cdots + a_nu_n = b_1u_1 + b_2u_2 + \cdots + b_nu_n$$

Then

$$0 = v - v = (a_1 - b_1)u_1 + (a_2 - b_2)u_2 + \cdots + (a_n - b_n)u_n$$

But since $\beta$ is linearly independent, we know that for all $i$, $a_i - b_i = 0$. Thus, $a_i = b_i$. Which gives uniqueness.

\[\square\]

**Theorem 1.9** If a vector space $V$ is generated by a finite set $S$, then some subset of $S$ is a basis for $V$. Hence $V$ has a finite basis.

**Proof.** If $S = \emptyset$ or $S = \{\emptyset\}$, then $V = \{\emptyset\}$ and $\emptyset$ is a subset of $S$ that is a basis for $V$. Otherwise $S$ contains a nonzero vector $u_1$. Technically, $\{u_1\}$ is a linearly independent set. Continue, if possible, choosing vectors $u_2, \ldots, u_k$ in $S$ such that $\{u_1, \ldots, u_k\}$ is linearly independent. Since $S$ is a finite set, we must eventually reach a stage at which $\beta = \{u_1, \ldots, u_k\}$ is a linearly independent subset of $S$, but adding any vector $v$ in $S$ to $\beta$ produces a linearly dependent set. We claim that $\beta$ is a basis for $V$. Because $\beta$ is linearly independent by construction, it suffices to show that $\beta$ spans $V$. That is, $\text{span}(\beta) = V$. 
Clearly, span(\(\beta\)) \(\subseteq\) \(V\), so we need only show that \(V \subseteq\) span(\(\beta\)).

We know that \(S \subseteq\) span(\(\beta\)). By Theorem 1.5 span(\(\beta\)) is a subspace. By Theorem 1.5 span(\(S\)) \(\subseteq\) span(\(\beta\)). But we know that span(\(S\)) = \(V\). Thus \(V \subseteq\) span(\(\beta\)).