Matt's Linear Algebra Notes

January 18, 2016

Chapter 1

Material

1.1 Vector Spaces

1.1.1 Introduction to Vector Spaces

Definition 1.1.1 (Vector Space)**.** A *vector space* V over a field $\mathbb{F}$ is a set with two binary operations, $+ : V \times V \to V$ and $\cdot : V \times \mathbb{F} \to V$ such that all of the following hold.

1. For all $x, y \in V$, $x + y = y + x$. (Additive Commutativity)
2. For all $x, y, z \in V$, $x + (y + z) = (x + y) + z$. (Additive Associativity)
3. There exists an element, denoted 0, in V such that for all $x \in V$, $x + 0 = x$.
4. For each $x \in V$ there exists a $y \in V$, denoted $-x$, such that $x + y = 0$.
5. For all $x \in V$, $1x = x$.
6. For all $a, b \in \mathbb{F}$ and $x \in V$, $a(bx) = (ab)x$.
7. For all $a \in \mathbb{F}$ and $x, y \in V$, $a(x + y) = ax + ay$.
8. For all $a, b \in \mathbb{F}$ and $x \in V$, $(a + b)x = ax + bx$.

Furthermore, $x + y$ is called the *sum of x and y* while ax is called the *product of x and a*. Moreover, each $x \in V$ is called a *vector* and each $a \in \mathbb{F}$ is called a *scalar*.

Definition 1.1.2 (n-tuple)**.** An object of the form $(a_1, a_2, \ldots, a_n)$ where $a_j \in \mathbb{F}$ for all $1 \le j \le n$, is called an *n-tuple*.

Example 1.1.1. *Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$, then $\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) | a_j \in \mathbb{F} \forall 1 \le j \le n\}$ forms a vector space under component-wise addition and multiplication as defined below for $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{F}^n$ and $k \in \mathbb{F}$.*

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$k(a_1, a_2, \ldots, a_n) = (ka_1, ka_2, \ldots, ka_n)$$

Furthermore, it said that

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$$

if and only if $a_j = b_j$ for all $1 \le j \le n$.

Proof. $\mathbb{F}^n$ is a vector space trivially from the fact that $\mathbb{F}$ is a field. □

Definition 1.1.3 (Matrix)**.** Let $\mathbb{F}$ be a field and $m, n \in \mathbb{N}$, then an $m \times n$ *matrix* with entries from $\mathbb{F}$ is a rectangular array of the form

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

where $a_{i,j} \in \mathbb{F}$ for all $1 \le i \le m$ and $1 \le j \le n$. The entries $(a_{i,1}, a_{i,2}, \ldots, a_{i,n})$ is called the *ith row* of the matrix and is a row vector in $\mathbb{F}^n$. The entries $(a_{1,j}, a_{2,j}, \ldots, a_{m,j})$ is called the *jth column* of the matrix and is a column vector in $\mathbb{F}^n$. We denote the entry on the ith row and jth column as $A_{i,j}$. Furthermore, two $m \times n$ matrices, A and B, are equal if and only if $A_{i,j} = B_{i,j}$ for all $1 \le i \le m$ and $1 \le j \le n$; we denote this by $A = B$. Moreover, if $n = m$ we say that A is a *square matrix*. Lastly, we denote the set of $m \times n$ matrices over $\mathbb{F}$ as $M_{m \times n}(\mathbb{F})$.

Example 1.1.2. *Let $\mathbb{F}$ be a field and $m, n \in \mathbb{N}$, then $M_{m\times n}(\mathbb{F})$ is a vector space over $\mathbb{F}$ under the following operations for $A, B \in M_{m\times n}(\mathbb{F})$ and $k \in \mathbb{F}$.*

$$(A+B)_{i,j} = A_{i,j} + B_{i,j}$$
$$(kA)_{i,j} = kA_{i,j}$$

Proof. The proof is trivial from the fact that we operating on multiple copies of a field. □

Example 1.1.3. *Let S be a nonempty set and let $\mathbb{F}$ be a field and let $\mathscr{F}(S, \mathbb{F})$ denote the set of all functions from S into $\mathbb{F}$. Two elements $f, g \in \mathscr{F}(S, \mathbb{F})$ are equal if and only if $f(s) = g(s)$ for all $s \in S$. Then $\mathscr{F}(S, \mathbb{F})$ is a vector space under the following operations for $f, g \in \mathscr{F}(S, \mathbb{F})$ and $k \in \mathbb{F}$.*

$$(f+g)(s) = f(s) + g(s)$$
$$(kf)(s) = k\,[f(s)]$$

Proof. The proof is trivial because all operations are done inside the field, and thus the space inherits the structure from $\mathbb{F}$. □

Definition 1.1.4 (Polynomial Ring)**.** Let $\mathbb{F}$ be a field. Then the *ring of polynomials in an indeterminate x over $\mathbb{F}$*, denoted $\mathbb{F}[x]$ is defined as

$$\mathbb{F}[x] := \{\sum_{i=0}^{n} a_i x^i | n \in \mathbb{N}, (a_0, a_1, \ldots, a_n) \in \mathbb{F}^n, a_n \neq 0\}.$$

Additionally, we define $x^0 = 1$. Moreover, for each $p = \sum_{i=0}^{n} p_i x^i \in \mathbb{F}[x]$, the *degree of p*, denoted $\deg p$, is n. Furthermore, if $p = 0$, that is $p_n = p_{n-1} = \ldots = p_0 = 0$, then p is called the *zero polynomial* and $\deg p = -1$ or $\deg p = -\infty$ depending on convention. If $\deg p = 0$, then we say p is a *constant polynomial.* Lastly, $\mathbb{F}[x]$ forms a ring under the following operations where $p, q \in \mathbb{F}[x]$ and without loss of generality assume, $\deg p \geq \deg q$.

$$p + q = \sum_{i=0}^{\deg q} (p_i + q_i)x^i + \sum_{i=\deg q+1}^{\deg p} p_i x^i$$
$$pq = \sum_{k=0}^{\deg p \cdot \deg q} \left(\sum_{i+j=k} p_i q_j \right) x^k$$

Example 1.1.4. *Let $\mathbb{F}$ be a field, then $\mathbb{F}[x]$ is a vector space over $\mathbb{F}$ under polynomial addition and scalar multiplication by constant polynomials.*

Proof. Since $\mathbb{F}[x]$ is a ring, it is closed under addition. Since constant polynomials are polynomials, it is closed under scalar multiplication. Since $\mathbb{F}[x]$ is a ring, addition is commutative and associative. Moreover the zero polynomial is the additive identity and likewise serves as the zero vector. Since $\mathbb{F}[x]$ is a ring, each $p \in \mathbb{F}[x]$ has a unique $-p \in \mathbb{F}[x]$ such that $p + (-p) = 0$. The constant polynomial 1 is the multiplicative identity in the ring and serves as the identity in the vector space. Furthermore, multiplication is associative and distributes over addition because $\mathbb{F}[x]$ is, indeed, a ring. □

Proposition 1.1.1. *If u, v, w are elements of a vector space V such that $x + z = y + z$ then, $x = y$.*

Proof. Since $z \in V$, then there exists a $-z \in V$ such that $z + (-z) = 0$. Thus, $x + z = y + z$ implies

$$x + z - z = y + z - z$$

and ergo $x = y$. □

Proposition 1.1.2. *The zero vector in any vector space V is unique.*

Proof. Assume there exists two zero vectors in V denoted 0_1 and 0_2. Then $v + 0_1 = v$ and $v + 0_2 = v$ for all $v \in V$. Therefore it is true that

$$0_2 = 0_2 + 0_1 = 0_1 + 0_2 = 0_1$$

and thus these identities are in fact the same. □

Proposition 1.1.3. *Let V be a vector space and let $v \in V$, then there exists a unique $u \in V$ such that $v + u = 0$.*

Proof. Assume v has two inverses, namely u_1 and u_2. Then $v + u_1 = 0$ and $v + u_2 = 0$. Therefore,

$$v + u_1 + u_2 = 0 + u_2 = u_2$$

and

$$v + u_1 + u_2 = v + u_2 + u_1 = 0 + u_1 = u_1.$$

Ergo, $u_1 = u_2$ and the inverse of v is unique. □

Proposition 1.1.4. *Let V be a vector space over a field $\mathbb{F}$, then:*

1. $0x = 0$ *for all* $x \in V$*;*
2. $a0 = 0$ *for all* $a \in \mathbb{F}$*;*
3. $(-a)x = -(ax) = a(-x)$ *for all* $x \in V$ *and* $a \in \mathbb{F}$*.*

Proof (1): Consider $0x + 0x$. Then,

$$0x + 0x = (0 + 0)x = 0x = 0 + 0x.$$

Since $0x + 0x = 0 + 0x$, by cancellation, we have $0x = 0$. □

Proof (2). Consider $a0 + a0$.

$$a0 + a0 = a(0 + 0) = a0 = a0 + 0$$

Thus, by cancellation, $a0 = 0$. □

Proof (3). Consider $-(ax)$. We know that $-(ax)$ is the unique additive inverse of ax, thus it is enough to show that $(-a)x$ and $a(-x)$ are inverses of ax.

$$\begin{aligned} ax + (-a)x &= (a - a)x \\ &= 0x \\ &= 0 \\ ax + a(-x) &= a(x - x) \\ &= a0 \\ &= 0 \end{aligned}$$

Thus $a(-x)$ and $(-a)x$ are inverses of ax and $(-a)x = -(ax) = a(-x)$. □

1.1.2 Subspaces

Definition 1.1.5 (Subspace)**.** A *subspace*, W, of a vector space, V, over a field, $\mathbb{F}$, is a subset of V that is also a vector space over $\mathbb{F}$.

Example 1.1.5. *For any vector space V, V and $\{0\}$ are subspaces of V. The latter is called the zero subspace.*

Theorem 1.1.5. *Let V be a vector space over a field $\mathbb{F}$ and let $W \subseteq V$. Then W is a subspace of V if and only if all of the following are satisfied.*

- $0 \in W$.
- *For all $x, y \in W$, $x + y \in W$.*
- *For all $a \in \mathbb{F}$ and $x \in W$, $ax \in W$.*

Proof. $\Rightarrow$ Since W is a subspace of V, $0 \in W$ and W is closed under V's vector addition and scalar multiplication.

$\Leftarrow$ Since V is a vector space W inherits associativity, commutativity, and distributivity from V as well as V's behavior with respect to the identities. Furthermore, $0 \in W$ by assumption. All that is left to show is that W contains additive inverses. Suppose $x \in W$, then by assumption $-x = (-1)x \in W$. Thus W is a subspace of V. $\square$

Definition 1.1.6 (Matrix Transpose)**.** Let M be an $m \times n$ matrix, then the *transpose of M*, denoted M^T, is the $n \times m$ matrix defined by $(M^T)_{i,j} = M_{j,i}$, that is

$$M^T = \begin{pmatrix} M_{1,1} & M_{2,1} & \dots & M_{m,1} \\ M_{1,2} & M_{2,2} & \dots & M_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ M_{1,n} & M_{2,n} & \dots & M_{m,n} \end{pmatrix}.$$

Definition 1.1.7 (Symmetric Matrix)**.** Let M be a matrix, then if $M = M^T$, we say M is *symmetric*.

Example 1.1.6. *The set of symmetric $n \times n$ matrices over a field $\mathbb{F}$, denoted $W_{n\times n}(\mathbb{F})$, is a subspace of $M_{n\times n}(\mathbb{F})$.*

Proof. Consider the zero matrix. Since the zero matrix is an $n \times n$ matrix with all entries equal to zero, the transpose of the zero matrix is also an $n \times n$ matrix with all entries equal to zero. Thus, $0 = 0^T$ and the zero matrix is symmetric.

Let $A, B \in W_{n\times n}(\mathbb{F})$. Then $A = A^T$ and $B = B^T$. By definition of symmetry and matrix transpose we have

$$A_{i,j} = (A^T)_{i,j} = A_{j,i} \tag{1.1}$$

and

$$B_{i,j} = (B^T)_{i,j} = B_{j,i} \tag{1.2}$$

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

Consider $(A + B)$. By definition we have

$$(A + B)_{i,j} = A_{i,j} + B_{i,j}.$$

By Equation 1.1 and Equation 1.2 we have

$$(A + B)_{i,j} = A_{i,j} + B_{i,j} = A_{j,i} + B_{j,i}.$$

The definition of matrix transpose implies that

$$(A+B)_{i,j} = A_{i,j} + B_{i,j} = A_{j,i} + B_{j,i} = (A^T)_{i,j} + (B^T)_{i,j}$$

and thus by definition of matrix addition,

$$(A+B)_{i,j} = A_{i,j} + B_{i,j} = A_{j,i} + B_{j,i} = (A^T)_{i,j} + (B^T)_{i,j} = (A^T + B^T)_{i,j}.$$

Ergo, $A+B$ is symmetric and $W(\mathbb{F})$ is closed under matrix addition.

Let $k \in \mathbb{F}$ and consider kA. We know by definition that

$$(kA)_{i,j} = k \cdot A_{i,j}.$$

We invoke Equation 1.1 again to get that

$$(kA)_{i,j} = k \cdot A_{i,j} = k \cdot A_{j,i}.$$

Applying the definition of matrix transpose yields,

$$(kA)_{i,j} = k \cdot A_{i,j} = k \cdot A_{j,i} = k \cdot (A^T)_{i,j}.$$

Lastly, by definition of scalar multiplication we have,

$$(kA)_{i,j} = k \cdot A_{i,j} = k \cdot A_{j,i} = k \cdot (A^T)_{i,j} = (kA^T)_{i,j}.$$

Thus kA is symmetric and $W(\mathbb{F})$ is closed under scalar multiplication. □

Definition 1.1.8 (Main Diagonal of a Matrix)**.** Let $\mathbb{F}$ be a field and let $M \in M_{n\times n}(\mathbb{F})$, then the *main diagonal of* M is the set $\{M_{i,i}\}_{i=1}^{n}$.

Definition 1.1.9 (Diagonal Matrix)**.** Let $\mathbb{F}$ be a field and let $A \in M_{n\times n}(\mathbb{F})$, then A is called a *diagonal matrix* if and only if whenever $i \neq j$, $A_{i,j} = 0$.

Example 1.1.7. *Let $\mathbb{F}$ be a field and let $D_n(\mathbb{F})$ be the set of all diagonal matrices in $M_{n\times n}(\mathbb{F})$, then $D_n(\mathbb{F})$ is a subspace on $M_{n\times n}(\mathbb{F})$.*

Proof. We know $0 \in D_n(\mathbb{F})$ since for all i,j, $0_{i,j} = 0$. Let $A, B \in D_n(\mathbb{F})$. Then for all $i \neq j$, $A_{i,j} = B_{i,j} = 0$. Thus, $(A+B)_{i,j} = A_{i,j} + B_{i,j} = 0 + 0 = 0$ whenever $i \neq j$ and $A+B$ is diagonal. Let $k \in \mathbb{F}$. Then $(kA)_{i,j} = k \cdot A_{i,j} = k \cdot 0 = 0$ and kA is diagonal. Therefore $D_n(\mathbb{F})$ forms a subspace of $M_{n\times n}(\mathbb{F})$. □

Definition 1.1.10 (Trace of a Matrix)**.** Let $\mathbb{K}$ be a field and let $M \in M_{n\times n}(\mathbb{K})$, then the *trace of* M denoted $\operatorname{tr} M$ is defined as

$$\operatorname{tr} M = \sum_{i=1}^{n} M_{i,i}$$

or the sum of the elements on the main diagonal.

Example 1.1.8. *Let $\mathbb{K}$ be a field and let $T_n(\mathbb{K})$ be the set of matrices in $M_{n\times n}(\mathbb{K})$ with trace equal to zero, then $T_n(\mathbb{K})$ is a subspace of $M_{n\times n}(\mathbb{K})$.*

Proof. Obviously, the zero matrix has a trace of zero and thus $0 \in T_n(\mathbb{K})$. Let $A, B \in T_n(\mathbb{K})$ then $\operatorname{tr} A = 0$ and $\operatorname{tr} B = 0$. Consider $\operatorname{tr}(A+B)$.

$$\operatorname{tr}(A+B) = \sum_{i=1}^{n} (A+B)_{i,i} = \sum_{i=1^n} (A_{i,i} + B_{i,i}) = \left(\sum_{i=1}^{n} A_{i,i}\right) + \left(\sum_{i=1}^{n} B_{i,i}\right) = \operatorname{tr} A + \operatorname{tr} B = 0$$

Thus, $A+B$ has trace 0 and $A+B \in T_n(\mathbb{K})$. Let $k \in \mathbb{K}$. Consider $\operatorname{tr}(kA)$.

$$\operatorname{tr}(kA) = \sum_{i=1}^{n} (kA)_{i,i} = \sum_{i=1}^{n} k \cdot A_{i,i} = k \sum_{i=1}^{n} A_{i,i} = k \operatorname{tr} A = 0$$

And thus, kA has trace 0 and $kA \in T_n(\mathbb{K})$. Therefore $T_n(\mathbb{K})$ is a subspace of $M_{n\times n}(\mathbb{K})$. □

Theorem 1.1.6. *Let V be a vector space over a field $\mathbb{F}$ and let $\mathcal{W}$ be a countable collection of subspaces of V. Then*

$$W_i = \bigcap_{W \in \mathcal{W}} W$$

is a subspace of V.

Proof. Since $0 \in W$ for all $W \in \mathcal{W}$, $0 \in W_i$. Let $x, y \in W_i$, then $x, y \in W$ for all $W \in \mathcal{W}$ and thus $x + y \in W$ for all $W \in \mathcal{W}$. Therefore, $x + y \in W_i$. Let $a \in \mathbb{F}$. Since $x \in W$ for all $W \in \mathcal{W}$, $ax \in W$ for all $W \in \mathcal{W}$. Ergo, $ax \in W_i$ and W_i is a subspace of V. □

Proposition 1.1.7. *For any matrix A, $[(A^T)^T] = A$.*

Proof. Apply the definition of matrix transposition twice.

$$[(A^T)^T]_{i,j} = (A^T)_{j,i} = A_{i,j}$$

□

Proposition 1.1.8. *For any matrix A, $A + A^T$ is symmetric.*

Proof. Consider $(A + A^T)_{i,j}$.

$$(A + A^T)_{i,j} = A_{i,j} + (A^T)_{i,j} = A_{i,j} + A_{j,i} = A_{j,i} + A_{i,j} = A_{j,i} + (A^T)_{j,i} = (A + A^T)_{j,i} = [(A + A^T)^T]_{i,j}$$

And thus, $(A + A^T)$ is symmetric. □

Proposition 1.1.9. *Let $\mathbb{K}$ be a field and let $A, B \in M_{n\times n}(\mathbb{K})$ and $a, b \in \mathbb{K}$, then $\operatorname{tr}(aA+bB) = a \operatorname{tr} A + b \operatorname{tr} B$.*

Proof.

$$\begin{aligned}
\operatorname{tr}(aA + bB) &= \sum_{i=1}^{n} (aA + bB)_{i,i} \\
&= \sum_{i=1}^{n} [(aA)_{i,i} + (bB)_{i,i}] \\
&= \left(\sum_{i=1}^{n} a \cdot A_{i,i} \right) + \left(\sum_{i=1}^{n} b \cdot B_{i,i} \right) \\
&= a \left(\sum_{i=1}^{n} A_{i,i} \right) + b \left(\sum_{i=1}^{n} B_{i,i} \right) \\
&= a \operatorname{tr} A + b \operatorname{tr} B
\end{aligned}$$

□

Definition 1.1.11 (Sum of Subsets of a Vector Space)**.** Let S, R be nonempty subsets of a vector space V, then the *sum of S and R*, denoted $S + R$ is defined as $S + R = \{s + r | s \in S, r \in R\}$.

Proposition 1.1.10. *Let U, W be subspaces of a vector space V over a field $\mathbb{F}$. Then $U + W$ is a subspace of V and is the smallest subspace containing both U and W.*

Proof. Since U and W are subspaces, $0 \in U$ and $0 \in W$ therefore, $0 = 0 + 0 \in U + W$. Let $x, y \in U + W$ then there exist $u_x, u_y \in U$ and $w_x, w_y \in W$ such that $x = u_x + w_x$ and $y = u_y + w_y$. Thus,

$$x + y = (u_x + w_x) + (u_y + w_y) = (u_x + u_y) + (w_x + w_y).$$

Since U and W are subspaces, $u_x + u_y \in U$ and $w_x + w_y \in W$. Ergo, $x + y = (u_x + u_y) + (w_x + w_y) \in U + W$.

Let $a \in \mathbb{F}$. Then,

$$ax = a(u_x + w_x) = au_x + aw_x.$$

Since U and W are subspaces, $au_x \in U$ and $aw_x \in W$. Ergo, $ax = au_x + aw_x \in U + W$ and $U + W$ is a subspace of V.

We know that, set-wise, $U = \{u + 0\}_{u \in U}$ and $W = \{0 + w\}_{w \in W}$, and thus $U, W \subseteq U + W$. Let X be a subspace of V such that $U, W \subseteq X$. Let $x \in U + W$, then there exists some $u \in U \subseteq X$ and $w \in W \subseteq X$ such that $x = u + w$. Therefore, $x = u + w \in X$ and $U + W \subseteq X$ for all subspaces X containing U and W. Ergo, $U + W$ is the smallest subspace of V containing U and W. □

Definition 1.1.12 (Direct Sum of Vector Spaces)**.** A vector space V is called the *direct sum of U and W*, denoted $V = U \oplus W$ if and only if U and W are subspaces of V such that $U \cap W = \emptyset$ and $U + W = V$.

Example 1.1.9. *Let $\mathbb{K}$ be a field and let $U = \{(a_1, a_2, \ldots, a_n) \in \mathbb{K}^n | a_n = 0\}$ and $V = \{(a_1, a_2 \ldots, a_n) \in \mathbb{K}^n | a_1 = a_2 = \ldots = a_{n-1} = 0\}$. Then $\mathbb{K}^n = U \oplus V$.*

Proof. The details are obvious and left as an exercise. □

Definition 1.1.13 (Cosets of a Vector Space)**.** Let U be a subspace of a vector space V over a field $\mathbb{K}$. Then for each $v \in V$ the set $\{v\} + W = \{v + w\}_{w \in W}$ is called the *coset of W containing v*, denoted $v + W$.

Proposition 1.1.11. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $v \in V$. Then $v + W$ is a subspace if and only if $v \in W$.*

Proof. $\Leftarrow$ Suppose $v \in W$. Then by closure, $v + W = \{v + w\}_{w \in W} = W$.

$\Rightarrow$ Suppose $v + W$ is a subspace of V. Then $0 \in v + W$ and therefore, there exists a $w \in W$ such that $0 = v + w$. This w can only be $-v$ by uniqueness of inverses. Since $-v \in W$, $v \in W$ since W is a subspace. □

Proposition 1.1.12. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $v \in V$. Then $v \in v + W$.*

Proof. Since W is a subspace, $0 \in W$ and thus $v = v + 0 \in v + W$. □

Proposition 1.1.13. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $u, v \in V$. Then $v + W \cap u + W = \emptyset$ if and only if $v + W \neq u + W$.*

Proof. $\Rightarrow$ Suppose $v + W \cap u + W = \emptyset$. Then since both $v + W$ and $u + W$ are non-empty, $v + W \neq u + W$.

$\Leftarrow$ Suppose $v + W \neq u + W$ with $v + W \cap u + W \neq \emptyset$. Then there exists an $x \in v + W \cap u + W$. Ergo, $x \in v + W$ and $x \in u + W$. Thus, there exists $w_1, w_2 \in W$ such that $x = v + w_1$ and $x = u + w_2$ respectively. Therefore, $v + w_1 = u + w_2$ and $v = u + w_2 - w_1$. Ergo,

$$v + W = \{v + w\}_{w \in W} = \{u + (w_2 - w_1 + w)\}_{w \in W} = u + W.$$

Thus, creating a contradiction. Therefore if $v + W \neq u + W$ then $v + W \cap u + W = \emptyset$. □

Proposition 1.1.14. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $u, v \in V$. Then $v + W = u + W$ if and only if $v - u \in W$.*

Proof. $\Rightarrow$ Assume $v + W = u + W$. Then $v \in v + W$ and thus $v \in u + W$. Ergo, there exists a $w \in W$ such that $v = u + w$. Solving for w yields $w = v - u \in W$.

$\Leftarrow$ Assume $v - u \in W$. Therefore, $u + v - u = v \in u + W$. We know $v \in v + W$ thus, $u + W \cap v + W \neq \emptyset$. This occurs if and only if $u + W = v + W$. □

Definition 1.1.14 (Quotient Space)**.** Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$. The the *quotient space of* V *modulo* W, denoted V/W is the set of all cosets of W,

$$V/W := \{v + W\}_{v \in V}.$$

Furthermore V/W is a vector space under the following operations.

$$\begin{aligned}(u + W) + (v + W) &= (u + v) + W \\ a(u + W) &= (au) + W\end{aligned}$$

Proof. A bunch of tedious symbol pushing that I refuse to do. $\square$

1.1.3 Linear Combinations

Definition 1.1.15 (Linear Combination)**.** Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. An $x \in V$ is said to be a *linear combination of elements of* S if and only if there exists a $\{s_j\}_{j=1}^n \subseteq S$ and scalars $\{a_j\}_{j=1}^n \subseteq \mathbb{F}$ where $n < \infty$ such that

$$x = \sum_{j=1}^n a_j y_j.$$

When this happens, we say x is a *linear combination of* $y_1, y_2, \ldots, y_n$.

Definition 1.1.16 (Spanning Set)**.** Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. Then, the *span of* S, denoted $\operatorname{span} S$, is the set

$$\operatorname{span} S = \{\sum_{j=1}^n a_j s_j | \{a_j\}_{j=1}^n \subseteq \mathbb{F}, \{s_j\}_{j=1}^n \subseteq S, n < \infty\}$$

or the set of linear combinations of elements of S. We define $\operatorname{span} \emptyset = \{0\}$.

Theorem 1.1.15. *Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. Then* $\operatorname{span} S$ *is a subspace of V and is the smallest subspace of V containing S.*

Proof. Let $\{s_j\}_{j=1}^n \subseteq S$ where $n < \infty$. Then $0 = \sum_{j=1}^n 0 s_j \in \operatorname{span} S$. Let $x, y \in \operatorname{span} S$. Then there exist $\{s_j\}_{j=1}^n, \{r_j\}_{j=1}^m \subseteq S$ and $\{a_j\}_{j=1}^n, \{b_j\}_{j=1}^m \subseteq \mathbb{F}$ with $m, n < \infty$ such that $x = \sum_{j=1}^n a_j s_j$ and $y = \sum_{j=1}^m b_j r_j$. Define $\{t_j\}_{j=1}^{n+m}$ and $\{c_j\}_{j=1}^{n+m}$ by

$$t_j = \begin{cases} s_j & j \leq n \\ r_j & j > n \end{cases} \qquad\qquad c_j = \begin{cases} a_j & j \leq n \\ b_j & j > n \end{cases}.$$

We can see that $\{t_j\}$ is a finite subset of S and $\{c_j\}$ is a finite subset of $\mathbb{F}$, thus any element made out of scalar multiples of t vectors is in $\operatorname{span} S$. Consider $x + y$.

$$x + y = \sum_{j=1}^n a_j s_j + \sum_{j=1}^m b_j r_j = \sum_{j=1}^n c_j t_j + \sum_{j=n+1}^{n+m} b_{j-n} r_{j-n} = \sum_{j=1}^n c_j t_j + \sum_{j=n+1}^{n+m} c_j t_j$$

Therefore, $x+y$ is a linear combination of elements of S and thus $x+y \in \operatorname{span} S$. Consider kx for any $k \in \mathbb{F}$.

$$kx = k \sum_{j=1}^n a_j s_j = \sum_{j=1}^n (k a_j) s_j$$

Ergo, $kx \in \operatorname{span} S$ and $\operatorname{span} S$ is a subspace of V.

Let W be a subspace of V such that $S \subseteq W$. Then for all $s \in S$ and $a \in \mathbb{F}$, $as \in W$ since W is a subspace. Ergo, for any $\{s_j\}_{j=1}^n \subseteq S$ and $\{a_j\}_{j=1}^n \subseteq \mathbb{F}$ with $n < \infty$

$$\sum_{j=1}^n a_j s_j \in W$$

since W is a subspace and any finite sum of vectors in W is in W. Ergo $\operatorname{span} S \subseteq W$ and is the smallest subspace of V containing S. ☐

Definition 1.1.17 (Span)**.** A subset S of a vector space V *spans* V if and only if $\operatorname{span} S = V$.

Example 1.1.10. *Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$. Define, $e_j := (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ where $a_j = 1$ and $a_i = 0$ for all $i \neq j$. Then $\{e_1, e_2, \ldots, e_n\}$ spans $\mathbb{F}^n$.*

Proof. Let $(c_1, c_2, \ldots, c_n) \in \mathbb{F}^n$. Then,

$$\sum_{j=1}^{n} c_j e_j = \sum_{j=1}^{n} (0, \ldots, c_j, \ldots, 0) = (c_1, c_2, \ldots, c_n) \in \operatorname{span}\{e_1, e_2, \ldots, e_n\}.$$

$\square$

Example 1.1.11. *Let $\mathbb{F}$ be a field and $n, m \in \mathbb{N}$. Define, $e_{i,j} \in M_{m\times n}(\mathbb{F}^n)$ where $(e_{i,j})_{i,j} = 1$ and $(e_{i,j})_{k,l} = 0$ for all $k \neq i$ and $j \neq l$. Then $\{e_{i,j}\}_{i,j=1}^{m,n}$ spans $M_{m\times n}(\mathbb{F}^n)$.*

Proof. Let $A \in M_{m\times n}(\mathbb{F}^n)$. Then,

$$\left(\sum_{i=1}^{m}\sum_{j=1}^{n} A_{i,j} e_{i,j}\right)_{k,l} = \sum_{i=1}^{m}\sum_{j=1}^{n} A_{i,j}(e_{i,j})_{k,l} = A_{k,l}$$

since $(e_{i,j})_{k,l} = 1$ when $i = k$ and $j = l$ and is zero otherwise. Thus,

$$A = \sum_{i=1}^{m}\sum_{j=1}^{n} A_{i,j} e_{i,j}.$$

$\square$

Proposition 1.1.16. *Let W be a nonempty subset of a vector space V over a field $\mathbb{F}$. Then W is a subspace of V if and only if $W = \operatorname{span} W$.*

Proof. $\Rightarrow$ Suppose W is a subspace. We know $W \subseteq \operatorname{span} W$, by definition. Furthermore, for all $w \in W$ and $a \in \mathbb{F}$, $aw \in W$ since W is a subspace. Thus, for any finite $\{w_j\}_{j=1}^n \subseteq W$ and $\{a_j\}_{j=1}^n \subseteq \mathbb{F}$, $\sum a_j w_j \in W$ by properties of vector spaces. Ergo, $\operatorname{span} W \subseteq W$ and $W = \operatorname{span} W$.

$\Leftarrow$ Suppose $W = \operatorname{span} W$. Since $\operatorname{span} W$ is a subspace and $W = \operatorname{span} W$, W is trivially a subspace. $\square$

Proposition 1.1.17. *Let S, R be nonempty subsets of V such that $S \subseteq R$. Then $\operatorname{span} S \subseteq \operatorname{span} R$ and if $\operatorname{span} S = V$, then $\operatorname{span} R = V$.*

Proof. I provide a sketch and leave the details to the reader.

All vectors in S are also in R ergo all sums of scalar multiples of vectors in S (read: $\operatorname{span} S$) are in $\operatorname{span} R$.

Furthermore, we know $\operatorname{span} R$ is a subspace of V, and thus $\operatorname{span} R \subseteq V$. If $V = \operatorname{span} S \subseteq \operatorname{span} R$, then $V \subseteq \operatorname{span} R$ and thus $\operatorname{span} R = V$. $\square$

1.1.4 Linear Independence

Definition 1.1.18 (Linear Independence)**.** A subset S of a vector space V over a field $\mathbb{F}$ is *linearly independent* if and only if for any $\{x_j\}_{j=1}^n \subseteq V$ where $n < \infty$ the statement

$$\sum_{j=1}^n a_j x_j = 0$$

implies that $\{a_j\} = \{0\}$, where $\{a_j\} \subseteq \mathbb{F}$. Furthermore, if S is not linearly independent, we say that S is *linearly dependent.*

Example 1.1.12. *Let $\mathbb{F}$ be a field and $n \in \mathbb{N}$. Define, $e_j := (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ where $a_j = 1$ and $a_i = 0$ for all $i \neq j$. Then $\{e_1, e_2, \ldots, e_n\}$ is linearly independent.*

Proof. Let $\{c_j\}_{j=1}^n \subseteq \mathbb{F}$ such that $\sum c_j e_j = 0$. Consider $c_j e_j$. On the jth entry of this vector, we will have c_j and all other entries are zero. Therefore,

$$\sum c_j e_j = (c_1, c_2, \ldots, c_n) = (0, 0, \ldots, 0).$$

By our definition of vector equality in $\mathbb{F}^n$ we have $c_j = 0$ for all $1 \leq j \leq n$. Thus, $\{e_j\}_{j=1}^n$ is linearly independent. □

Example 1.1.13. *Let $\mathbb{F}$ be a field and $n, m \in \mathbb{N}$. Define, $e_{i,j} \in M_{m\times n}(\mathbb{F}^n)$ where $(e_{i,j})_{i,j} = 1$ and $(e_{i,j})_{k,l} = 0$ for all $k \neq i$ and $j \neq l$. Then $\{e_{i,j}\}_{i,j=1}^{m,n}$ is linearly independent.*

Proof. Let $\{a_{i,j}\}_{i,j=1}^{m,n} \subseteq \mathbb{F}$ such that $\sum\sum a_{i,j} e_{i,j} = 0$. Then, for all $1 \leq k \leq m$ and $1 \leq l \leq n$

$$0 = \left(\sum\sum a_{i,j} e_{i,j}\right)_{k,l} = \sum\sum a_{i,j}(e_{i,j})_{k,l} = a_{k,l}.$$

Thus, $\{a_{i,j}\} = \{0\}$ and $\{e_{i,j}\}_{i,j=1}^{m,n}$ is linearly independent. □

Theorem 1.1.18. *A subset S of a vector space V over a field $\mathbb{F}$ is linearly dependent if and only if $x_1 = 0$ or there exists a $k < n$ such that $x_{k+1} \in \operatorname{span}\{x_1, x_2, \ldots, x_k\}$.*

Proof. $\Rightarrow$ Assume S is linearly dependent. Therefore, there exists a $\{a_j\}_{j=1}^n \subseteq \mathbb{F}$ with $\{a_j\}_{j=1}^n \neq \{0\}$ such that $\sum a_j x_j = 0$. Define $k = \max\{j | a_j \neq 0\}$. If $1 < k \leq n$, then

$$\sum_{j=1}^n a_j x_j = \sum_{j=1}^k a_j x_j = 0$$

and

$$x_k = \sum_{j=1}^n (-a_j a_k^{-1}) \in \operatorname{span}\{x_1, x_2, \ldots, x_{k-1}\}.$$

If $k = 1$, then

$$\sum_{j=1}^n a_j x_j = a_1 x_1 = 0$$

with $a_1 \neq 0$. Ergo, $x_1 = 0$.

$\Leftarrow$ Assume $x_1 = 0$. Then $ax_1 = 0$ for all $a \in \mathbb{F}$ and S is linearly dependent. Assume there exists a $k < n$ such that $x_{k+1} \in \operatorname{span}\{x_1, x_2, \ldots, x_k\}$. Then there exists $\{a_j\} \subseteq \mathbb{F}$ such that $x_{k+1} = \sum_{j=1}^k a_j x_j$. We know $\sum_{j=1}^k a_j x_j - x_{k+1}$ is a linear combination of vectors in $\mathbb{F}$ and

$$\sum_{j=1}^k a_j x_j - x_{k+1} = 0$$

thus, S is linearly dependent. □

1.1.5 Bases and Dimension

Definition 1.1.19 (Basis of a Vector Space)**.** A *basis* B for a vector space V is a a linearly independent subset of V that spans V.

Example 1.1.14. *Let* $\mathbb{F}$ *be a field and* $n \in \mathbb{N}$*. Define,* $e_j := (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ *where* $a_j = 1$ *and* $a_i = 0$ *for all* $i \neq j$*. Then* $\{e_1, e_2, \ldots, e_n\}$ *is a basis of* $\mathbb{F}^n$*.*

Example 1.1.15. *Let* $\mathbb{F}$ *be a field and* $n, m \in \mathbb{N}$*. Define,* $e_{i,j} \in M_{m\times n}(\mathbb{F}^n)$ *where* $(e_{i,j})_{i,j} = 1$ *and* $(e_{i,j})_{k,l} = 0$ *for all* $k \neq i$ *and* $j \neq l$*. Then* $\{e_{i,j}\}_{i,j=1}^{m,n}$ *is a basis of* $M_{m\times n}(\mathbb{F}^n)$*.*

Proof. We proved that both of the above examples are linearly independent and span their vector spaces in the linear independence and linear combination sections respectively. Thus, they are both bases of their respective vector spaces. $\square$

Theorem 1.1.19. *Let* S *be a linearly independent subset of a vector space* V *over a field* $\mathbb{F}$ *and* $x \in V \setminus S$*. Then,* $S \cup \{x\}$ *is linearly dependent if and only if* $x \in \operatorname{span} S$*.*

Proof. $\Rightarrow$ Suppose $S \cup \{x\}$ is linearly dependent. Ergo, there exists a $\{s_i\}_{i=1}^n \subseteq S \cup \{x\}$ and $\{a_i\}_{i=1}^n \subseteq \mathbb{F} \setminus \{0\}$ such that

$$\sum a_i s_i = 0.$$

Furthermore, $x \in \{s_i\}$ since if $x \notin \{s_i\}$ then $\{s_i\} \subseteq S$, which is linearly independent. Without loss of generality, suppose $x = s_n$. Thus,

$$\sum a_i s_i + a_n s_n = 0$$

and

$$x = s_n = -a_n^{-1} \sum a_i s_i \in \operatorname{span} S.$$

$\Leftarrow$ Suppose $x \in \operatorname{span} S$. Then there exists $\{s_i\}_{i=1}^n \subseteq S$ and $\{a_i\}_{i=1}^n \subseteq \mathbb{F} \setminus \{0\}$ such that

$$x = \sum a_i s_i.$$

Therefore,

$$\sum a_i s_i + (-1)x = 0$$

and $S \cup \{x\}$ is linearly dependent. $\square$

Theorem 1.1.20. *Let* V *be a vector space over a field* $\mathbb{K}$*. If* V *is spanned by a finite subset,* S*, then a subset of* S *is a basis for* V*. Therefore,* V *has a finite basis.*

Proof. If $S = \emptyset$ or $S = \{0\}$. then trivially, $V = \{0\}$ and we found our basis, congrats. Otherwise, we have the more interesting case where there exists at least one $x_1 \in S$ with $x_1 \neq 0$. Note, that the set $\{x_1\}$ is linearly independent. If possible, continue picking elements $x_2, x_3, \ldots, x_n$ such that $B = \{x_1, x_2, \ldots, x_n\}$ is linearly independent until adding any other element causes B to be linearly dependent or we run out of elements. If we ran out of elements while constructing our linearly independent subset, then S is linearly independent and thus is a finite basis of V, yay. Otherwise, for any $y \in S \setminus B$, we know that $B \cup \{y\}$ is linearly dependent and thus, $y \in \operatorname{span} B$. Moreover, $B \subseteq \operatorname{span} B$. Ergo, $S \subseteq \operatorname{span} B \subseteq \operatorname{span} S$. However, since $\operatorname{span} S$ is the minimal subspace of V containing S and $\operatorname{span} B$ is also a subspace, $\operatorname{span} S \subseteq \operatorname{span} B$ and $\operatorname{span} B = \operatorname{span} S$. Thus, B is a linearly independent subset that spans V. Finally, we can say B is a finite basis of V since $B \subseteq S$, a finite set. $\square$

Theorem 1.1.21. *Let* V *be a vector space over a field* $\mathbb{F}$ *with a basis,* B*, containing* n *elements. Let* $S = \{y_1, y_2, \ldots, y_m\}$ *be a linearly independent subset of* V *with* $m \leq n$*. Then there exists a subset* B_1 *in* B *with cardinality* $n - m$ *such that* $S \cup B_1$ *is a basis* V*.*

Proof. Proceed via induction on m. Let $H(k)$ represent that the hypothesis that the theorem is true for $m = k$. Consider $H(0)$. In this case, $S = \emptyset$ and taking $B_1 = B$ satisfies the theorem. Suppose $H(k)$ is true for some $k < n$, we now wish to show that $H(k+1)$ is true. Let $S := \{y_1, y_2, \ldots, s_{k+1}\}$ be linearly independent. Since S is linearly independent, $S' := \{y_1, \ldots, y_k\}$ is linearly independent. Since $H(k)$ is true, there exists a $B' := \{x_1, \ldots, x_{n-k}\} \subseteq B$ such that $S' \cup B'$ spans V. Therefore, there exists $\{a_j\}_{j=1}^{k}, \{b_j\}_{j=1}^{n-k} \subseteq \mathbb{F}$ such that

$$y_{k+1} = \left(\sum_{j=1}^{k} a_j y_j\right) + \left(\sum_{j=1}^{n-k} b_j x_j\right). \tag{1.3}$$

Furthermore, at least one b_j must be nonzero, because otherwise,

$$y_{k+1} = \sum_{j=1}^{k} a_j y_j$$

a clear violation of our assumed linear independence. Without loss of generality, assume b_1 is nonzero. Take $B_1 = B' \setminus \{x_1\}$. Solving Equation 1.3 for x_1 yields,

$$x_1 = \left(\sum_{j=1}^{k} b_1^{-1} a_j y_j\right) + \left(\sum_{j=2}^{n-k} b_1^{-1} b_j x_j\right) - b_1^{-1} y_{k+1}$$

which is clearly in the span of $S \cup B_1$. Furthermore, $y_1, \ldots, y_m, y_{m+1}, x_2, \ldots, x_{n-k}$ is also in that span. By minimality (Theorem 1.1.15), we have

$$\operatorname{span}(S' \cup B') \subseteq \operatorname{span}(S \cup B_1) \subseteq V.$$

However, $\operatorname{span}(S' \cup B') = V$ by $H(K)$ and thus,

$$V \subseteq \operatorname{span}(S \cup B_1) \subseteq V.$$

Ergo, $\operatorname{span}(S \cup B_1) = V$. Since $S \cup B_1$ is linearly independent as well, $S \cup B_1$ is a basis. □

Corollary 1.1.22. *Let V be a vector space over a field $\mathbb{F}$ with a basis B that contains n elements. Then any linearly independent subset of V with cardinality n is a basis for V.*

Proof. Let $S \subseteq V$ be linearly independent with $\operatorname{card} S = n$. Then by Theorem 1.1.21 there exists a $B_1 \subseteq B$ with $\operatorname{card} B_1 = n - n = 0$ such that $B_1 \cup S$ is a basis for V. Since $\operatorname{card} B_1 = 0$, $B_1 = \emptyset$ and S is a basis for V. □

Corollary 1.1.23. *Let V be a vector space over a field $\mathbb{F}$ that has a basis, B, with $\operatorname{card} B = n$. Then any subset of V with cardinality greater than n is linearly dependent.*

Proof. Suppose $S \subseteq V$ is linearly independent with $\operatorname{card} S > n$. Therefore any $R \subset S$ with $\operatorname{card} R = n$ is a basis of V. Moreover, since $\operatorname{card} R < \operatorname{card} S$ and $R \subset S$, there exists an $x \in S \setminus R$. Since R is a basis, and $x \in V$, $x \in \operatorname{span} R$, which in turn tells us that S is linearly dependent. Therefore, any $S \subseteq V$ with $\operatorname{card} S > n$ is linearly dependent. □

Corollary 1.1.24. *Let V be a vector space over a field $\mathbb{F}$ that has a basis, B, with $\operatorname{card} B = n$. Then any basis of V contains exactly n elements*

Proof. Suppose S is a basis of V. Since B is a basis, it is linearly independent and thus it has cardinality less than or equal to n. Define $m = \operatorname{card} S$. We know that $m \leq n$ since S is linearly independent and B is a basis. Moreover, $nleqm$ since B is linearly independent and S is a basis. Thus, $m = n$ and any basis of V will have cardinality n. □

Definition 1.1.20 (Dimension of a Vector Space)**.** A vector space V is called *finite-dimensional* if and only if V has a finite basis. Furthermore B is a basis of V with $\operatorname{card} B = n$ then we say V has *dimension* n, denoted $\dim V = n$. If V is not finite-dimensional, then we say V is *infinite-dimensional*.

Corollary 1.1.25. *Suppose V is a vector space with $\dim V = n$ and let $S \subseteq V$ span V with $\operatorname{card} S \leq n$. Then S is a basis of V.*

Proof. Since $\operatorname{span} S = V$, there exists an $S' \subseteq S$ such that S' is a basis for V. Since S' is a basis and $\dim V = n$, $\operatorname{card} S' = n$. Thus,

$$n = \operatorname{card} S' \leq \operatorname{card} S \leq n.$$

Yielding, $\operatorname{card} S = n$ and $S' = S$. Therefore, S is a basis of V. $\square$

Corollary 1.1.26. *Let B be a basis for a finite-dimensional vector space V and let $S \subseteq V$ be linearly independent. Then there exists a $B' \subseteq B$ such that $B' \cup S$ is a basis of V.*

Proof. Define $\dim V = n$ and $\operatorname{card} S = m \leq n$. Then by replacement theorem, there exists a $B' \subseteq B$ with $\operatorname{card} B' = n - m$ such that $B' \cup S$ is a basis of V. $\square$

Theorem 1.1.27. *Let W be a subspace of a finite dimensional vector space V. Then W is finite dimensional and $\dim W \leq \dim V$. Moreover, if $\dim W = \dim V$, then $W = V$.*

Proof. Let B be a basis for W. Then B is linearly independent. Since B is linearly independent and $B \subseteq W \subseteq V$, $\dim W = \operatorname{card} B \leq \dim V$.

Suppose $\dim W = \dim V$. Let B be a basis for W. Since B is linearly independent and $\operatorname{card} B = \dim W = \dim V$, B is a basis for V. Thus, $W = \operatorname{span} B = V$. $\square$

Corollary 1.1.28. *Let W be a subspace of a finite dimensional vector space V, then any basis of W is a subset of a basis of V.*

Proof. Let S be a basis of W and B be a basis of V. Then S is linearly independent and by replacement theorem there exists a $B' \subseteq B$ such that $S \cup B'$ is a basis of V. Obviously, $S \subseteq S \cup B'$ and thus S is a subset of a basis of V. $\square$

Chapter 2

Definitions

2.1 Vector Spaces

2.1.1 Introduction to Vector Spaces

Definition 2.1.1 (Vector Space)**.** A *vector space* V over a field $\mathbb{F}$ is a set with two binary operations, $+ : V \times V \to V$ and $\cdot : V \times \mathbb{F} \to V$ such that all of the following hold.

1. For all $x, y \in V$, $x + y = y + x$. (Additive Commutativity)
2. For all $x, y, z \in V$, $x + (y + z) = (x + y) + z$. (Additive Associativity)
3. There exists an element, denoted 0, in V such that for all $x \in V$, $x + 0 = x$.
4. For each $x \in V$ there exists a $y \in V$, denoted $-x$, such that $x + y = 0$.
5. For all $x \in V$, $1x = x$.
6. For all $a, b \in \mathbb{F}$ and $x \in V$, $a(bx) = (ab)x$.
7. For all $a \in \mathbb{F}$ and $x, y \in V$, $a(x + y) = ax + ay$.
8. For all $a, b \in \mathbb{F}$ and $x \in V$, $(a + b)x = ax + bx$.

Furthermore, $x + y$ is called the *sum of x and y* while ax is called the *product of x and a*. Moreover, each $x \in V$ is called a *vector* and each $a \in \mathbb{F}$ is called a *scalar*.

Definition 2.1.2 (n-tuple)**.** An object of the form $(a_1, a_2, \ldots, a_n)$ where $a_j \in \mathbb{F}$ for all $1 \leq j \leq n$, is called an *n-tuple*.

Definition 2.1.3. Let $\mathbb{F}$ be a field and $m, n \in \mathbb{N}$, then an $m \times n$ *matrix* with entries from $\mathbb{F}$ is a rectangular array of the form

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{pmatrix}$$

where $a_{i,j} \in \mathbb{F}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. The entries $(a_{i,1}, a_{i,2}, \ldots, a_{i,n})$ is called the *ith row* of the matrix and is a row vector in $\mathbb{F}^n$. The entries $(a_{1,j}, a_{2,j}, \ldots, a_{m,j})$ is called the *jth column* of the matrix and is a column vector in $\mathbb{F}^n$. We denote the entry on the ith row and jth column as $A_{i,j}$. Furthermore, two $m \times n$ matrices, A and B, are equal if and only if $A_{i,j} = B_{i,j}$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$; we denote this by $A = B$. Moreover, if $n = m$ we say that A is a *square matrix*. Lastly, we denote the set of $m \times n$ matrices over $\mathbb{F}$ as $M_{m \times n}(\mathbb{F})$.

Definition 2.1.4 (Polynomial Ring)**.** Let $\mathbb{F}$ be a field. Then the *ring of polynomials in an indeterminate x over* $\mathbb{F}$, denoted $\mathbb{F}[x]$ is defined as

$$\mathbb{F}[x] := \{\sum_{i=0}^{n} a_i x^i | n \in \mathbb{N}, (a_0, a_1, \ldots, a_n) \in \mathbb{F}^n, a_n \neq 0\}.$$

Additionally, we define $x^0 = 1$. Moreover, for each $p = \sum_{i=0}^{n} p_i x^i \in \mathbb{F}[x]$, the *degree of p*, denoted $\deg p$, is n. Furthermore, if $p = 0$, that is $p_n = p_{n-1} = \ldots = p_0 = 0$, then p is called the *zero polynomial* and $\deg p = -1$ or $\deg p = -\infty$ depending on convention. If $\deg p = 0$, then we say p is a *constant polynomial.*

Lastly, $\mathbb{F}[x]$ forms a ring under the following operations where $p, q \in \mathbb{F}[x]$ and without loss of generality assume, $\deg p \geq \deg q$.

$$p + q = \sum_{i=0}^{\deg q} (p_i + q_i)x^i + \sum_{i=\deg q+1}^{\deg p} p_i x^i$$

$$pq = \sum_{k=0}^{\deg p \cdot \deg q} \left(\sum_{i+j=k} p_i q_j \right) x^k$$

2.1.2 Subspaces

Definition 2.1.5 (Subspace)**.** A *subspace*, W, of a vector space, V, over a field, $\mathbb{F}$, is a subset of V that is also a vector space over $\mathbb{F}$.

Definition 2.1.6 (Matrix Transpose)**.** Let M be an $m \times n$ matrix, then the *transpose of* M, denoted M^T, is the $n \times m$ matrix defined by $(M^T)_{i,j} = M_{j,i}$, that is

$$M^T = \begin{pmatrix} M_{1,1} & M_{2,1} & \dots & M_{m,1} \\ M_{1,2} & M_{2,2} & \dots & M_{m,2} \\ \vdots & \vdots & \ddots & \vdots \\ M_{1,n} & M_{2,n} & \dots & M_{m,n} \end{pmatrix}.$$

Definition 2.1.7 (Symmetric Matrix)**.** Let M be a matrix, then if $M = M^T$, we say M is *symmetric.*

Definition 2.1.8 (Main Diagonal of a Matrix)**.** Let $\mathbb{F}$ be a field and let $M \in M_{n\times n}(\mathbb{F})$, then the *main diagonal of* M is the set $\{M_{i,i}\}_{i=1}^n$.

Definition 2.1.9 (Diagonal Matrix)**.** Let $\mathbb{F}$ be a field and let $A \in M_{n\times n}(\mathbb{F})$, then A is called a *diagonal matrix* if and only if whenever $i \neq j$, $A_{i,j} = 0$.

Definition 2.1.10 (Trace of a Matrix)**.** Let $\mathbb{K}$ be a field and let $M \in M_{n\times n}(\mathbb{K})$, then the *trace of* M denoted $\operatorname{tr} M$ is defined as

$$\operatorname{tr} M = \sum_{i=1}^{n} M_{i,i}$$

or the sum of the elements on the main diagonal.

Definition 2.1.11 (Sum of Subsets of a Vector Space)**.** Let S, R be nonempty subsets of a vector space V, then the *sum of* S *and* R, denoted $S + R$ is defined as $S + R = \{s + r | s \in S, r \in R\}$.

Definition 2.1.12 (Direct Sum of Vector Spaces)**.** A vector space V is called the *direct sum of* U *and* W, denoted $V = U \oplus W$ if and only if U and W are subspaces of V such that $U \cap W = \emptyset$ and $U + W = V$.

Definition 2.1.13 (Cosets of a Vector Space)**.** Let U be a subspace of a vector space V over a field $\mathbb{K}$. Then for each $v \in V$ the set $\{v\} + W = \{v + w\}_{w\in W}$ is called the *coset of* W *containing* v, denoted $v + W$.

Definition 2.1.14 (Quotient Space)**.** Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$. The the *quotient space of* V *modulo* W, denoted V/W is the set of all cosets of W,

$$V/W := \{v + W\}_{v\in V}.$$

Furthermore V/W is a vector space under the following operations.

$$\begin{aligned} (u + W) + (v + W) &= (u + v) + W \\ a(u + W) &= (au) + W \end{aligned}$$

2.1.3 Linear Combinations

Definition 2.1.15 (Linear Combination)**.** Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. An $x \in V$ is said to be a *linear combination of elements of* S if and only if there exists a $\{s_j\}_{j=1}^n \subseteq S$ and scalars $\{a_j\}_{j=1}^n \subseteq \mathbb{F}$ where $n < \infty$ such that

$$x = \sum_{j=1}^{n} a_j y_j.$$

When this happens, we say x is a *linear combination of* $y_1, y_2, \ldots, y_n$.

Definition 2.1.16 (Spanning Set)**.** Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. Then, the *span of* S, denoted $\operatorname{span} S$, is the set

$$\operatorname{span} S = \{\sum_{j=1}^{n} a_j s_j | \{a_j\}_{j=1}^n \subseteq \mathbb{F}, \{s_j\}_{j=1}^n \subseteq S, n < \infty\}$$

or the set of linear combinations of elements of S. We define $\operatorname{span} \emptyset = \{0\}$.

Definition 2.1.17 (Span)**.** A subset S of a vector space V *spans* V if and only if $\operatorname{span} S = V$.

2.1.4 Linear Independence

Definition 2.1.18 (Linear Independence)**.** A subset S of a vector space V over a field $\mathbb{F}$ is *linearly independent* if and only if for any $\{x_j\}_{j=1}^n \subseteq V$ where $n < \infty$ the statement

$$\sum_{j=1}^{n} a_j x_j = 0$$

implies that $\{a_j\} = \{0\}$, where $\{a_j\} \subseteq \mathbb{F}$. Furthermore, if S is not linearly independent, we say that S is *linearly dependent.*

2.1.5 Bases and Dimension

Definition 2.1.19 (Basis of a Vector Space)**.** A *basis* B for a vector space V is a a linearly independent subset of V that spans V.

Definition 2.1.20 (Dimension of a Vector Space)**.** A vector space V is called *finite-dimensional* if and only if V has a finite basis. Furthermore B is a basis of V with $\operatorname{card} B = n$ then we say V has *dimension* n, denoted $\dim V = n$. If V is not finite-dimensional, then we say V is *infinite-dimensional*.

Chapter 3

Theorems

3.1 Vector Spaces

3.1.1 Introduction to Vector Spaces

Proposition 3.1.1. *If u, v, w are elements of a vector space V such that $x + z = y + z$ then, $x = y$.*

Proposition 3.1.2. *The zero vector in any vector space V is unique.*

Proposition 3.1.3. *Let V be a vector space and let $v \in V$, then there exists a unique $u \in V$ such that $v + u = 0$.*

Proposition 3.1.4. *Let V be a vector space over a field $\mathbb{F}$, then:*

1. $0x = 0$ *for all* $x \in V$;
2. $a0 = 0$ *for all* $a \in \mathbb{F}$;
3. $(-a)x = -(ax) = a(-x)$ *for all* $x \in V$ *and* $a \in \mathbb{F}$.

3.1.2 Subspaces

Theorem 3.1.5. *Let V be a vector space over a field $\mathbb{F}$ and let $W \subseteq V$. Then W is a subspace of V if and only if all of the following are satisfied.*

- $0 \in W$.
- *For all $x, y \in W$, $x + y \in W$.*
- *For all $a \in \mathbb{F}$ and $x \in W$, $ax \in W$.*

Theorem 3.1.6. *Let V be a vector space over a field $\mathbb{F}$ and let $\mathcal{W}$ be a countable collection of subspaces of V. Then*

$$W_i = \bigcap_{W \in \mathcal{W}} W$$

is a subspace of V.

Proposition 3.1.7. *For any matrix A, $[(A^T)^T] = A$.*

Proposition 3.1.8. *For any matrix A, $A + A^T$ is symmetric.*

Proposition 3.1.9. *Let $\mathbb{K}$ be a field and let $A, B \in M_{n\times n}(\mathbb{K})$ and $a, b \in \mathbb{K}$, then $\operatorname{tr}(aA+bB) = a \operatorname{tr} A + b \operatorname{tr} B$.*

Proposition 3.1.10. *Let U, W be subspaces of a vector space V over a field $\mathbb{F}$. Then $U + W$ is a subspace of V and is the smallest subspace containing both U and W.*

Proposition 3.1.11. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $v \in V$. Then $v + W$ is a subspace if and only if $v \in W$.*

Proposition 3.1.12. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $v \in V$. Then $v \in v + W$.*

Proposition 3.1.13. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $u, v \in V$. Then $v + W \cap u + W = \emptyset$ if and only if $v + W \neq u + W$.*

Proposition 3.1.14. *Let $\mathbb{K}$ be a field and W be a subspace of a vector space V over $\mathbb{F}$ and let $u, v \in V$. Then $v + W = u + W$ if and only if $v - u \in W$.*

3.1.3 Linear Combinations

Theorem 3.1.15. *Let V be a vector space over a field $\mathbb{F}$ and let S be a nonempty subset of V. Then* $\operatorname{span} S$ *is a subspace of V and is the smallest subspace of V containing S.*

Proposition 3.1.16. *Let W be a nonempty subset of a vector space V over a field $\mathbb{F}$. Then W is a subspace of V if and only if $W = \operatorname{span} W$.*

Proposition 3.1.17. *Let S, R be nonempty subsets of V such that $S \subseteq R$. Then* $\operatorname{span} S \subseteq \operatorname{span} R$ *and if* $\operatorname{span} S = V$*, then* $\operatorname{span} R = V$*.*

3.1.4 Linear Independence

Theorem 3.1.18. *A subset S of a vector space V over a field $\mathbb{F}$ is linearly dependent if and only if $x_1 = 0$ or there exists a $k < n$ such that $x_{k+1} \in \operatorname{span}\{x_1, x_2, \ldots, x_k\}$.*

3.1.5 Bases and Dimension

Theorem 3.1.19. *Let S be a linearly independent subset of a vector space V over a field $\mathbb{F}$ and $x \in V \setminus S$. Then, $S \cup \{x\}$ is linearly dependent if and only if $x \in \operatorname{span} S$.*

Theorem 3.1.20. *Let V be a vector space over a field $\mathbb{K}$. If V is spanned by a finite subset, S, then a subset of S is a basis for V. Therefore, V has a finite basis.*

Theorem 3.1.21. *Let V be a vector space over a field $\mathbb{F}$ with a basis, B, containing n elements. Let $S = \{y_1, y_2, \ldots, y_m\}$ be a linearly independent subset of V with $m \leq n$. Then there exists a subset B_1 in B with cardinality $n - m$ such that $S \cup B_1$ is a basis V.*

Corollary 3.1.22. *Let V be a vector space over a field $\mathbb{F}$ with a basis B that contains n elements. Then any linearly independent subset of V with cardinality n is a basis for V.*

Corollary 3.1.23. *Let V be a vector space over a field $\mathbb{F}$ that has a basis, B, with $\operatorname{card} B = n$. Then any subset of V with cardinality greater than n is linearly dependent.*

Corollary 3.1.24. *Let V be a vector space over a field $\mathbb{F}$ that has a basis, B, with $\operatorname{card} B = n$. Then any basis of V contains exactly n elements*

Corollary 3.1.25. *Suppose V is a vector space with $\dim V = n$ and let $S \subseteq V$ span V with $\operatorname{card} S \leq n$. Then S is a basis of V.*

Theorem 3.1.26. *Let W be a subspace of a finite dimensional vector space V. Then W is finite dimensional and $\dim W \leq \dim V$. Moreover, if $\dim W = \dim V$, then $W = V$.*