Linear Algebra

Jayadev Naram

June 4, 2020

Contents

1 Spaces*

{*Add it as a chapter} {*Increase the line width}

1.1 Dimension

Definition 1. *A **field** is a set $\mathbb{F}$ together with two binary operations $\{+, \cdot\}$ on $\mathbb{F}$ called addition and multiplication respectively. To every pair $\alpha, \beta \in \mathbb{F}$, there corresponds an element $\alpha + \beta, \alpha \cdot \beta \in \mathbb{F}$, called the sum and product respectively. These operations satisfy the following axioms called the field axioms. For any $\alpha, \beta, \gamma \in \mathbb{F}$,*

- *i) (Associative Laws of Addition and Multiplication)*
  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, and $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

- *ii) (Commutative Laws of Addition and Multiplication)*
  $\alpha + \beta = \beta + \alpha$, and $\alpha \cdot \beta = \beta \cdot \alpha$.

- *iii) (Distributive Law of Multiplication over Addition)*
  $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.

- *iv) (Additive and Multiplicative identity) There exist two different elements 0 and 1 in $\mathbb{F}$ such that $\alpha + 0 = \alpha$ and $\alpha \cdot 1 = \alpha$.*

- *v) (Additive inverses) For every $\alpha \in \mathbb{F}$, there exists an element in $\mathbb{F}$, denoted $-\alpha$, called the additive inverse of α, such that $\alpha + (-\alpha) = 0$.*

- *vi) (Multiplicative inverses) For every $\alpha \neq 0$ in $\mathbb{F}$, there exists an element in F, denoted by α^{-1} or $\dfrac{1}{\alpha}$, called the multiplicative inverse of α, such that $\alpha \cdot \alpha^{-1} = 1$.*

From now on we call the elements of a field as scalars.

Definition 2. *A **vector space** over a field $\mathbb{F}$ is a set V together with two operations addition and scalar multiplication. To every pair $x, y \in V$, there corresponds an element $x + y \in V$, called the sum of x and y and to every pair $x \in V$ and $\alpha \in \mathbb{F}$, there corresponds an element $\alpha x \in V$. These operations satisfy the following axioms. For any $x, y, z \in V$ and $\alpha, \beta \in \mathbb{F}$ any scalars,*

- *i) (Commutative Law of Addition) $x + y = y + x$.*

- *ii) (Associative Law of Addition) $x + (y + z) = (x + y) + z$*

- *iii) (Additive identity) There exists a unique vector 0 in V(called the origin) such that $x + 0 = x \, \forall \, x \in V$*

- *iv) (Additive inverses) To every vector x in V there corresponds a unique vector -x such that $x + (-x) = O$.*

- *v) (Associative Law of Scalar Multiplication) $\alpha(\beta x) = (\alpha\beta)x$*

- *vi) (Distributive Law of Multiplication over Scalar and Vector Addition)*
  a) With respect to vector addition, $\alpha(x + y) = \alpha x + \alpha y$.
  b) With respect to scalar addition, $(\alpha + \beta)x = \alpha x + \beta x$.

vii) $1x = x$ *for every vector x.*

Definition 3. *A set $\{x_1, \cdots, x_n\}$ of vectors is **linearly dependent** if there exists a corresponding set $\{a_i\}$ of scalars, not all zero, such that $\Sigma_i \alpha_i x_i = 0$, in other words,*

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \implies \exists\, k \in \{1, \cdots, n\} \text{ such that } \alpha_k \neq 0. \tag{1}$$

On the otherhand, if

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \implies \alpha_i = 0 \,\forall\, i \in \{1, \cdots, n\}, \tag{2}$$

*then the set is **linearly independent**.*

Note 1. *For a set of vectors $\{x_1, \cdots, x_n\}$ if $x_k = 0$ for some $k, 1 \leq k \leq n$, then $\sum_{i=1}^{n} \alpha_i x_i = 0 \implies \alpha_k \neq 0$. Thus $\{x_1, \cdots, x_n\}$ is linearly dependent if atleast one of the vectors is a zero vector.*

Definition 4. *A vector x is said to be a **linear combination** of the set of vectors $\{x_1, \cdots, x_n\}$, if $x = \sum_{i=1}^{n} \alpha_i x_i$.*

Lemma 1. *The set of non-zero vectors $\{x_1, \cdots, x_n\}$ is linearly dependent if and only if some vector is a linear combination of the remaining vectors.*

Proof. Suppose the set of nonzero vectors $\{x_1, \cdots, x_n\}$ is linearly dependent. Then we have

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \implies \text{ not all } \alpha_i \text{ are zero.} \tag{3}$$

If only one of the scalars is non-zero, say $\alpha_k \neq 0$ then it follows from (3) that $\alpha_k x_k = 0 \implies x_k = 0$, which is a contradiction since we assumed all the vectors in the set to be non-zero. Then we have atleast two scalars non-zero and now from (3)

$$x_k = \frac{-\alpha_1}{\alpha_k} x_1 + \cdots + \frac{-\alpha_{k-1}}{\alpha_k} x_{k-1} + \frac{-\alpha_{k+1}}{\alpha_k} x_{k+1} + \cdots + \frac{-\alpha_n}{\alpha_k} x_n, \tag{4}$$

where $\alpha_k \neq 0$ and $\alpha_i \neq 0$, for $i \neq k, 1 \leq i \leq n$.

We now prove the converse. WLOG suppose x_n is a linear combination of $x_1, \cdots, x_{n-1}$ then we prove that $x_1, \cdots, x_n$ is linearly dependent. Let $x_n = \sum_{i=1}^{n-1} \beta_i x_i$, then not all β_i are zero since $x_1, \cdots, x_n$ are all nonzero vectors. So we have

$$-\beta_1 x_1 - \cdots - \beta_{n-1} x_{n-1} + x_n = 0,$$

where atleast one β_i is non zero. Thus by Definition 3, we see that $x_1, \cdots, x_n$ is linearly dependent. $\qquad\square$

Definition 5. *A **basis** in a vector space V is a set $X \subset V$ of linearly independent vectors such that every vector in V is a linear combination of elements of X. A vector space V is **finite-dimensional** if it has a finite basis.*

Remark 1. *Every vector x in V can be expressed in one and only way as a linear combination of basis vectors, since if $x = \sum_i \alpha_i x_i = \sum_i \beta_i x_i$, then we have $\sum_i (\alpha_i - \beta_i) x_i = 0$ and now by linear independence of $\{x_i\}$ we conclude that $\alpha_i = \beta_i, \forall i$.*

Lemma 2. *Let $S = \{x_1, \cdots, x_n\}$ be a basis for a vector space V and y be any non-zero vector in V. Then some $x_k \in S$ is a linear combination of $S_1 = \{y, x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n\}$ and S_1 is also a basis for V.*

Proof. Consider the set
$$S' = \{y, x_1, \cdots, x_n\}.$$

First notice that every vector in V is a linear combination of vectors of S', but such combinations may not be unique. In fact, since y is nonzero, it follows from Lemma 1 that S' is a linearly dependent set of vectors and y can be written as a linear combination of S, say $y = \sum_{i=1}^{n} \alpha_i x_i$ where atleast one scalar must be nonzero, say α_k. Then we have

$$y = \sum_{i=1}^{n} \alpha_i x_i \implies x_k = \beta_0 y + \sum_{i=1, i \neq k}^{n} \beta_i x_i, \tag{5}$$

where $\beta_0 = \dfrac{-1}{\alpha_k}$ and $\beta_i = \dfrac{-\alpha_i}{\alpha_k}$, $1 \leq i \leq n$. The above expression gives us the explicit linear combination of x_k in terms of the remaining vectors of S'. Consider the set
$$S_1 = \{y, x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n\}.$$

We proceed to prove that S_1 is also a basis for V using the fact that S is a basis for V. To show that S_1 is linearly independent set of vectors, consider the following:

$$\gamma_0 y + \sum_{i=1, i \neq k}^{n} \gamma_i x_i = 0. \tag{6}$$

Then, we have

$$\gamma_0 \sum_{i=1}^{n} \alpha_i x_i + \sum_{i=1, i \neq k}^{n} \gamma_i x_i = 0 \implies \gamma_0 \alpha_k x_k + \sum_{i=1, i \neq k}^{n} (\gamma_0 \alpha_i + \gamma_i) x_i = 0$$

$$\implies \sum_{i=1}^{n} \gamma_i' x_i = 0, \text{ where } \gamma_k' = \gamma_0 \alpha_k \text{ and } \gamma_i' = \gamma_0 \alpha_i + \gamma_i \ \forall i, 1 \leq i \leq n, i \neq k.$$

Since S is basis, it is linearly independent, i.e, $\gamma_i' = 0 \ \forall i, 1 \leq i \leq n$. In particular, $\gamma_k' = 0$, i.e, $\gamma_0 \alpha_k = 0 \implies \gamma_0 = 0$ since $\alpha_k \neq 0$. Then, for $i \neq k, 0 = \gamma_i' = \gamma_i$. Since (6) $\implies \gamma_i = 0 \ \forall i, 0 \leq i \leq n, i \neq k$ we can conclude that S_1 is linearly independent set of vectors.

Now to prove that every vector in V is a linear combination of vectors of S_1, write any vector u in V as linear combination of vectors of S(basis) and then replace x_k by the linear combination (5). So any vector u in V is a linear combination of vectors of S_1. Thus S_1 is a basis for V. $\qquad \square$

Lemma 3. *If $S = \{x_1, \cdots, x_n\}$ is a basis for a vector space V and if $\{y_1, \cdots, y_m\}$ is any set of linearly independent vectors in V, then*

4

(a) $m \leq n$; and

(b) unless the y's already form a basis, we can find vectors $y_{m+1}, \cdots, y_{m+p}$ so that $\{y_1, \cdots, y_m, y_{m+1}, \cdots y_{m+p}\}$, is a basis. In other words, every linearly independent set can be extended to a basis.

Proof. Suppose in contrary to the assertion (a) that $m > n$. Consider the set $S'_1 = \{y_1, x_1, \cdots, x_n\}$. By Lemma 2, we find a vector $x_k \in S'_1$ which is a linear combination of remaining vectors of S'_1 and

$$S_1 = \{y_1, x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n\}$$

is also a basis for V. Now construct S_2 by adding y_2 and removing some x_j. S_2 is also a basis for V. Then continuing this process for n-1 times (this is possible since $m > n$), we are left with the set

$$S_{n-1} = \{y_1, \cdots, y_{n-1}, x_i\}, 1 \leq i \leq n,$$

which is also a basis for V. Following the above process, we remove x_i and add y_n and the resultant set

$$S_n = \{y_1, \cdots, y_{n-1}, y_n\}$$

is also a basis for V. Since $m > n$, y_{n+1} exists and since S_n is basis, y_{n+1} can will be a linear combination of S_n or y's, which is a contradiction. Hence, $m \leq n$, i.e, y's are exhausted first and the last set is

$$S_m = \{y_1, \cdots, y_m, x_{i_1}, \cdots, x_{i_{n-m}}\}, \text{ where } i_l \in \{1, \cdots, n\}.$$

This last set S_n is a basis for V and contains the linearly independent set of vectors $\{y_1, \cdots, y_m\}$. □

Theorem 4. *The number of elements in any basis of a finite-dimensional vector space V is the same as in any other basis.*

Proof. Let $S = \{x_1, \cdots, x_n\}$ and $T = \{y_1, \cdots, y_m\}$ both be bases for V. Consider S to be the basis and T as a linearly independent set of vectors in V, then it follows from Lemma 3 that $m \leq n$. Now by reversing the above argument we have $n \leq m$, thus $m = n$. □

Definition 6. *The **_dimension_** of a finite-dimensional vector space V is the number of elements in a basis of V.*

Corollary 4.1. *Every set of $n+1$ vectors in an n-dimensional vector space V is linearly dependent.*

Proof. Follows from Theorem 4 and Lemma 3 □

1.2 Subspaces

Definition 7. *A non-empty subset M of a vector space V is a **_subspace_** or a **_linear manifold_** if $x, y \in M$, then $\alpha x + \beta y \in M$, for any scalars α, β.*

Remark 2. *Any subspace M must contain the zero vector since if $x \in M$, then $0x \in M$, i.e, $0 \in M$.*

Lemma 5. *The intersection of any class of subspaces of a vector space V is a subspace of V.*

Proof. Let $\{M_i\}$ be an arbitrary class of subspaces of V indexed by a set J. Denote by M the intersection of the class of subspaces, i.e,

$$M = \bigcap_{i \in J} M_i = \{x \mid x \in M_i \ \forall \ i \in J\}.$$

Since zero vector belongs to every subspace M_i, $0 \in M$, so M is non-empty. Now suppose $x, y \in M$, then $x, y \in M_i \ \forall \ i \in J$. But $\alpha x + \beta y \in M_i \ \forall \ i \in J$, which means $\alpha x + \beta y \in M$. $\qquad\square$

Lemma 6. *If S is any set of vectors in a vector space V and if M^* is the smallest subspace containing S, then M^* is the same as the set of all linear combinations of elements of S.*

Proof. Let M' denote the set of all linear combinations of elements of S. Observe that $0 \in M'$ and it is clear that a linear combination of linear combinations of elements of S can again be written as a linear combination of elements of S. Hence the M' is a subspace of V containing S and since M^* is the smallest subspace containing S, it follows that $M^* \subseteq M'$.

Now notice that since M^* is a smallest subspace containing S, for every collection of elements in S, their linear combination belong to M^*, so every element of M' belongs to M^*. Thus $M' = M^*$. $\qquad\square$

Definition 8. *The **_span_** of an arbitrary subset S of a vector space, denoted by span(S), is the smallest subspace containing S or equivalently the subspace containing all the linear combinations of elements of S.*

Remark 3. *In this new terminology, we see that a basis X for a vector space V is a linearly independent set of vectors whose span is V, i.e, span(X) = V.*

Theorem 7. *A subspace M in an n-dimensional vector space V is a vector space of dimension $\leq n$.*

Proof. If $M = \{0\}$, then M is 0-dimensional, and we are done. If M contains a nonzero vector x_1, define a set $X = \{x_1\}$. Then either of two will hold: i) $M = span(X)$, in which case M is 1-dimensional and we are done; ii) $M \neq span(X)$, in which case we find another nonzero vector x_2, such that $x_2 \notin span(X)$ and then we proceed as above after appending x_2 to X and repeating the process. By Corollary 4.1(Section 1.1), we know that the above process will terminate after n+1 steps, since $n + 1$ vectors cannot be linearly independent. $\qquad\square$

Corollary 7.1. *Given any m-dimensional subspace M in an n-dimensional vector space V, we can find a basis $\{x_1, \cdots, x_m, x_{m+1}, \cdots, x_n\}$ in V so that $x_1, \cdots, x_m$ are in M and thus, form a basis of M.*

Proof. Follows from Theorem 7 and Lemma 3 (Section 1.1). $\qquad\square$

Definition 9. *Let H and K be any two subspaces of V, then by $H+K$ we mean the subspace spanned by H and K together, i.e, $H+K = span(\{X_H, X_K\})$, where X_H and X_K are bases of H and K respectively. We shall say that a subspace K of a vector space V is a **_complement_** of a subspace H if*

$$H \cap K = \{0\} \ and \ H + K = V.$$

Note 2. *Consider a non-trivial subspace M of V, i.e, $\{0\} \subset M \subset V$. Let N be a complement of M. Then pick nonzero elements m, n from M and N respectively. Then consider a basis X of N including n. Define a new set $X' = X \cup \{n + m\} \setminus \{n\}$ and notice that $span(X') \equiv N' \neq N$, $M \cap N' = \{0\}(??)$ and $M + N' = V$. So N' is another complement of M, different from N. Therefore, for any non-trivial subspace M of V, i.e, $\{0\} \subset M \subset V$, there exists more than one complement.*

Theorem 8. *If M is an m-dimensional subspace in an n-dimensional vector space V, then every complement of M has dimension $n - m$.*

Proof. It is sufficient to prove the assertion for any one complement of M, then by Note 2 it should hold for every complement, since each of the complements of M have same number of basis elements.

By Corollary 7.1, we can find a basis of V such that first m elements form the basis for M. Then the subspace spanned by the remaining $n - m$ basis vectors is a complement of M and it is an $n - m$ dimensional subspace of V. $\qquad \square$

1.3   Isomorphism

Definition 10. *Consider two vector spaces U and V over the same field. We say U is **isomorphic** to V if there is a bijection T between U and V which preserves linear relations, i.e,*

$$\forall x_1, x_2 \in U, \ T(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 T(x_1) + \alpha_2 T(x_2).$$

*In other words, U and V are **isomorphic** if there is an isomorphism (such as T) between them.*

Theorem 9. *Every n-dimensional vector space V over a field $\mathbb{F}$ is isomorphic to $\mathbb{F}^n$.*

Proof. Let $\{x_1, \cdots, x_n\}$ be any basis in V. Each x in V can be written in the form $\xi_1 x_1 + \cdots + \xi_n x_n$. Consider the map $x \mapsto (\xi_1, \cdots, \xi_n)$. Since for each x in V, $(\xi_1, \cdots, \xi_n)$ is uniquely determined by Remark 1, this is bijection. It also preserves linear relations since if $x_1 \mapsto (\xi_1, \cdots, \xi_n)$ and $x_2 \mapsto (\zeta_1, \cdots, \zeta_n)$, then $\alpha_1 x_1 + \alpha_2 x_2 \mapsto \alpha_1 (\xi_1, \cdots, \xi_n) + \alpha_2 (\zeta_1, \cdots, \zeta_n)$. $\qquad \square$

1.4   Direct Sum

Definition 11. *If U and V are vector spaces (over the same field), then the **direct sum** of U and V is the vector space W, denoted by $U \oplus V$, whose elements are all the ordered pairs (x, y) with x in U and y in V, with the linear operations defined by*

$$\alpha_1 (x_1, y_1) + \alpha_2 (x_2, y_2) = (\alpha_1 x_1 + \alpha_2 x_2, \alpha_1 y_1 + \alpha_2 y_2).$$

Note 3. *We can view the direct sum, $W = U \oplus V$ as the cartesian product $U \times V$ which is given a vector space structure, i.e, defining linear operations(vector sum and scalar multiplication). In this interpretation, it can be seen that $U \times \{0\}$ is a subspace of $U \oplus V$ since it contains vectors of the form $(x, 0), x \in U$ and $(\alpha x + \beta y, 0) = \alpha(x, 0) + \beta(y, 0)$. Also notice that $\forall \ x \in U$, the map $(x, 0) \mapsto x$*

is an isomorphism, thus $U \times \{0\}$ is isomorphic to U. Similarly, $\{0\} \times V$ is a subspace of $U \oplus V$ and is isomorphic to V. In regard to these isomorphisms between vector spaces, if we denote the elements of the direct sum (u,v) by $u+v$, then we may identify U, V as subspaces of $U \oplus V$.

Theorem 10. *If U and V are subspaces of a vector space W, then the following three conditions are equivalent.*

i) $W = U \oplus V$

ii) $U \cap V = \{0\}$ and $U + V = W$ (i.e, U and V are complements of each other)

iii) *Every vector z in W may be written in the form $z = x + y$, with x in U and y in V, in one and only one way.*

Proof. We shall prove the implications $i) \implies ii) \implies iii) \implies i)$.

$i) \implies ii)$. We assume that $W = U \oplus V$. If $z = (x, y)$ lies in both U and V, then x = y = 0, so that z = 0; this proves that $U \cap V = \{0\}$. Since the representation $z = (x, 0) + (0, y)$ is valid for every z, it follows also that $U + V = W$.

$ii) \implies iii)$. If we assume $U + V = W$, then it is clear that every z in W has the desired representation, $z = x + y$. To prove uniqueness, we assume that $z = x_1 + y_1 = x_2 + y_2$, where $x_1, x_2 \in U$ and $y_1, y_2 \in V$. Then it follows that $x_1 - x_2 = y_1 - y_2$. Since the left member of this last equation is in U and the right member is in V, the disjointness of direct sum implies that $x_1 = x_2$ and $y_1 = y_2$.

$iii) \implies i)$. This is equivalent to the Definition 11 due to the notation introduced in Note 3. $\square$

Theorem 11. $dim(U \oplus V) = dim(U) + dim(V)$.

Proof. Consider a basis for U and V as follows: $\{x_1, \cdots, x_n\}, \{y_1, \cdots, y_m\}$ respectively and define that set $S = \{x_1, \cdots, x_n, y_1, \cdots, y_m\}$. Since every vector in $U \oplus V$ can be written as $z = x + y$, where $x \in U$ and $y \in V$, we conclude that $U \oplus V = span(S)$. To show that S is linearly independent set of vectors, consider

$$\sum_{i=1}^{n} \alpha_i x_i + \sum_{j=1}^{m} \beta_j y_j = 0.$$

Since the zero vector of the right hand side is a vector in the direct sum which can be uniqely written as $x + y$, where $x = \sum_{i=1}^{n} \alpha_i x_i$ and $y = \sum_{j=1}^{m} \beta_j y_j$, we have

$$\sum_{i=1}^{n} \alpha_i x_i = 0 \text{ and } \sum_{j=1}^{m} \beta_j x_j = 0.$$

Since $\{x_1, \cdots, x_n\}, \{y_1, \cdots, y_m\}$ are basis of U and V respectively, we only have trivial solution to the above equation. $\square$

Theorem 12. *If W is any $(n + m)$-dimensional vector space, and if U is any n-dimensional subspace of W, then there exists an m-dimensional subspace V in W such that $W = U \oplus V$.*

Proof. Let $\{x_1, \cdots, x_n\}$ be any basis in U; by the Lemma 3 (Section 1.1) we may find a set $\{y_1, \cdots, y_m\}$ of vectors in W with the property that

$$\{x_1, \cdots, x_n, y_1, \cdots, y_m\}$$

is a basis in W. Let V be the subspace spanned by $\{y_1, \cdots, y_m\}$, then it can be seen that $U \cap V = \{0\}$ and also that $U + V = W$. $\qquad\square$

1.5 Dual Spaces

Definition 12. *A **linear functional** on a vector space V is a scalar-valued function y defined for every vector x in V, with the property that*

$$y(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 y(x_1) + \alpha_2 y(x_2), \ \forall x_1, x_2 \in V, \ \text{and any scalars } \alpha_1, \alpha_2.$$

Note 4. *Let y be any linear functional on a vector space V, then $y(0) = 0$, since $y(0) = y(0 \cdot 0) = 0 \cdot y(0) = 0$.*

Remark 4. *For any two linear functionals y_1, y_2 on a vector space V define $y(x) = y_1(x) + y_2(x)$. Then for any $x_1, x_2 \in V$ and any scalars α_1, α_2, we have*

$$
\begin{aligned}
y(\alpha_1 x_1 + \alpha_2 x_2) &= y_1(\alpha_1 x_1 + \alpha_2 x_2) + y_2(\alpha_1 x_1 + \alpha_2 x_2) \\
&= (\alpha_1 y_1(x_1) + \alpha_2 y_1(x_2)) + (\alpha_1 y_2(x_1) + \alpha_2 y_2(x_2)) \\
&= \alpha_1(y_1(x_1) + y_2(x_1)) + \alpha_2(y_1(x_2) + y_2(x_2)) \\
&= \alpha_1 y(x_1) + \alpha_2 y(x_2).
\end{aligned}
$$

For any linear functional y_1 on V and scalar α define $y(x) = \alpha y_1(x)$. Then for any $x_1, x_2 \in V$ and any scalars α_1, α_2, we have

$$
\begin{aligned}
y(\alpha_1 x_1 + \alpha_2 x_2) &= \alpha y_1(\alpha_1 x_1 + \alpha_2 x_2) = \alpha(\alpha_1 y_1(x_1) + \alpha_2 y_1(x_2)) \\
&= \alpha_1(\alpha y_1(x_1)) + \alpha_2(\alpha y_1(x_2)) = \alpha_1 y(x_1) + \alpha_2 y(x_2).
\end{aligned}
$$

Therefore, if y_1, y_2 are linear functionals on V and α any scalar, then $y_1 + y_2$ and αy_1 are also a linear functional on V. Also note that the functional y defined as $y(x) = 0 \ \forall x \in V$ is a linear functional on V.

Definition 13. *The **dual space** of V, denoted by V', is the set of all linear functionals on V. By the Remark 4, we can define the following on V'*

  i) *the addition of $y_1, y_2 \in V'$ as an element $y \in V'$ (denoted by $y_1 + y_2$), such that $y(x) = y_1(x) + y_2(x), \ \forall x \in V$;*

  ii) *the scalar multiplication of y_1 with the scalar α as an element $y \in V'$, such that $y(x) = \alpha y_1(x), \ \forall x \in V$;*

  iii) *let $0 \in V'$, defined as $0(x) = 0 \ \forall x \in V$, play the role of additive identity.*

The dual space V' together with i), ii), iii) forms a vector space of all linear functionals on V.

Note 5 (Change in Notation)**.** *We make a change in notation of representing the output of linear functionals. Suppose y is a linear functional on a vector space V and x is any vector in V, then instead of denoted the output of y when x*

is given as input as $y(x)$ we represent it with $[x, y]$. So from now on $[x, y] \equiv y(x)$. In terms of the symbol $[x, y]$ the defining property of a linear functional is

$$[\alpha_1 x_1 + \alpha_2 x_2, y] = \alpha_1[x_1, y] + \alpha_2[x_2, y], \tag{7}$$

and the definition of the linear operations for linear functionals is

$$[x, \alpha_1 y_1 + \alpha_2 y_2] = \alpha_1[x, y_1] + \alpha_2[x, y_2]. \tag{8}$$

*The two relations together are expressed by saying that $[x, y]$ is a **bilinear functional** of the vectors x in V and y in V'.*

Lemma 13. *If V is an n-dimensional vector space, if $\{x_1, \cdots, x_n\}$ is a basis in V, and if $\{a_1, \cdots, a_n\}$ is any set of n scalars, then there is one and only one linear functional y on V such that $[x_i, y] = a_i \ \forall i, 1 \le i \le n$.*

Proof. Let x be a vector in V such that $x = \sum_{i=1}^{n} \xi_i x_i$ and consider the functional y defined by

$$[x, y] = \sum_{i=1}^{n} \xi_i \alpha_i.$$

Consider another vector in V $x' = \sum_{i=1}^{n} \zeta_i x_i$, then

$$
\begin{aligned}
{[\beta_1 x + \beta_2 x', y]} &= \left[\sum_{i=1}^{n} (\beta_1 \xi_i + \beta_2 \zeta_i) x_i, y \right] = \sum_{i=1}^{n} (\beta_1 \xi_i + \beta_2 \zeta_i) \alpha_i \\
&= \beta_1 \sum_{i=1}^{n} \xi_i \alpha_i + \beta_2 \sum_{i=1}^{n} \zeta_i \alpha_i = \beta_1[x, y] + \beta_2[x', y].
\end{aligned}
$$

This shows y is a linear functional on V. Notice that $[x_i, y] = \alpha_i$. This shows the existence of the linear functional satisfying the properties mentioned in the assertion.

Now we prove the uniqness of such linear functional. Suppose on the contrary that there exist two linear functionals y_1, y_2 on V such that $[x_i, y_1] = \alpha_i = [x_i, y_2] \ \forall i, 1 \le i \le n$. Then for any vector x in V with $x = \sum_{i=1}^{n} \xi_i x_i$, we have

$$[x, y_1] = \sum_{i=1}^{n} \xi_i \alpha_i = [x, y_2] \implies [x, y_1 - y_2] = 0 \ \forall x \in V \implies y_1 = y_2.$$

This proves the uniqness. $\square$

Theorem 14. *If V is an n-dimensional vector space and if $X = \{x_1, \cdots, x_n\}$ is a basis in V, then there is a uniquely determined basis X' in V', $X' = \{y_1, \cdots, y_n\}$, with the property that $[x_i, y_i] = \delta_{ij}$. Consequently the dual space of an n-dimensional space is n-dimensional. The basis X' is called the **dual basis** of X.*

Proof. By Lemma 13 it follows that $\forall j, 1 \le j \le n$, there exists a unique $y_j \in V'$ such that $[x_i, y_j] = \delta_{ij} \ \forall i, 1 \le i \le n$. So we only need to prove that the set $X' = \{y_1, \cdots, y_n\}$ is a basis for V'.

To show that X' is linearly independent set, consider $\alpha_1 y_1 + \cdots + \alpha_n y_n = 0$. Then, $\forall x \in V$, we have

$$0 = [x, \alpha_1 y_1 + \cdots + \alpha_n y_n] = \alpha_1[x, y_1] + \cdots + \alpha_n[x, y_n].$$

The above equation must also hold for $x = x_i$, then

$$0 = \alpha_1[x_i, y_1] + \cdots + \alpha_n[x_i, y_n] = \alpha_i.$$

So, $\alpha_1 y_1 + \cdots + \alpha_n y_n \implies \alpha_1 = \cdots = \alpha_n = 0$, hence X' is linearly independent.

Now we prove that $span(X') = V'$. Consider a linear functional y defined as $[x_i, y] = \alpha_i$, then for $x = \sum_{i=1}^n \xi_i x_i$, we have $[x, y] = \sum_{i=1}^n \xi_i \alpha_i$. On the otherhand, $[x, y_j] = \xi_j$, so substituting this in the preceding equation, we get

$$[x, y] = \alpha_1[x, y_1] + \cdots + \alpha_n[x, y_n] = [x, \alpha_1 y_1 + \cdots + \alpha_n y_n].$$

Thus, any linear functional $y = \sum_{j=1}^n \alpha_j y_j$. $\qquad\square$

Corollary 14.1. *If u and v are any two different vectors of the n-dimensional vector space V, then there exists a linear functional y on V such that $[u, y] \neq [v, y]$; or, equivalently, to any non-zero vector x in V there corresponds a y in V' such that $[x, y] \neq 0$.*

Proof. First notice that both the statements are indeed equivalent since we can consider $0 \neq x = u - v$.

Let $X = \{x_1, \cdots, x_n\}$ be any basis for V, and let $X' = \{y_1, \cdots, y_n\}$ be the dual basis for V'. If $x = \sum_{i=1}^n \xi_i x_i$, then from the proof of Theorem 14, we have $[x, y_j] = \xi_j$. Now suppose on the contrary that for $x \neq 0$ and $\forall y \in V'$, $[x, y] = 0$ then this should hold for $y = y_j$, i.e, $[x, y_j] = 0 = \xi_j$, then $x = 0$ which is a contradiction. $\qquad\square$

Theorem 15. *If V is a finite-dimensional vector space, then corresponding to every linear functional z_0 on V' there is a vector x_0 in V such that $z_0(y) = [x_0, y] = y(x_0)$ for every y in V'; the map $x_0 \mapsto z_0$ between V and V'' is an isomorphism. The correspondence described in this statement is called the* ___natural correspondence___ *between V and V''.*

Proof. Consider the map $x_0 \mapsto z_0$, such that to every $x_0 \in V$ we have a $z_0 \in V''$ defined by $z_0(y) = y(x_0) \; \forall y \in V'$. Suppose for $x_1, x_2 \in V$ and $z_1, z_2 \in V''$ we have $x_1 \mapsto z_1$ and $x_2 \mapsto z_2$, then for any two scalars α_1, α_2 and $\forall y \in V'$ we have

$$[\alpha_1 x_1 + \alpha_2 x_2, y] = \alpha_1[x_1, y] + \alpha_2[x_2, y] = \alpha_1[y, z_1] + \alpha_2[y, z_2] = [y, \alpha_1 z_1 + \alpha_2 z_2].$$

This shows that $\alpha_1 x_1 + \alpha_2 x_2 \mapsto \alpha_1 z_1 + \alpha_2 z_2$, thus this map is linear.

Now we prove that this map is one-to-one, i.e, if for $x_1, x_2 \in V$ and $z_1, z_2 \in V''$ we have $x_1 \mapsto z_1$ and $x_2 \mapsto z_2$ then $z_1 = z_2 \implies x_1 = x_2$. Suppose $z_1 = z_2$, then $[x_1, y] = [x_2, y] \; \forall y \in V'$. Then by Corollary 14.1, we have $x_1 = x_2$.

Now we prove that the map is a bijection. Notice that since the map $x_0 \mapsto z_0$ is one-to-one and linear, we can say that the range set of this map is a subspace of V'' of dimension equal to $dim(V)$. But now applying Theorem 14, we see that the dimension of V'' is equal to the dimension of V', which is again equal to the dimension of V, i.e, $dim(V'') = dim(V') = dim(V)$, which makes the map, onto. Therefore, the map $x_0 \mapsto z_0$ is isomorphism from V to V''. $\qquad\square$

Note 6. *The Theorem 15 not just shows that V and V'' are isomorphic, but more importantly it shows that the natural correspondence $x_0 \mapsto z_0$, defined by $z_0(y) = [x_0, y] = y(x_0)$ for every y in V', is an isomorphism. This property of vector spaces is called* ___reflexivity___.

Therefore, ___every finite-dimensional vector space is reflexive.___

Note 7 (Change in notation). *For finite-dimensional vector spaces we shall identify V'' with V (by the natural isomorphism), and we shall say that the element z_0 of V'' is the same as the element x_0 of V whenever $z_0(y) = [x_0, y]$ $\forall y \in V'$. In this language it is very easy to express the relation between a basis X for V and the dual basis of its dual basis for V''; the symmetry of the relation $[x_i, y_j] = \delta_{ij}$ shows that $X'' = X$.*

Definition 14. *The __annihilator__ S^0 of any subset S of a vector space V (S need not be a subspace)is the set of all vectors y in V' such that $[x, y]$ is identically zero $\forall x \in S$.*

Remark 5. *Notice that $\{0\}^0 = V'$, since $\forall y \in V', [0, y] = 0$. Similarly, $V^0 = \{0\}(\subset V')$, since the only linear functional that is identically zero on every vector of V is zero functional. If V is finite-dimensional and S contains a nonzero vector, so that $S \neq \{0\}$, then by Corollary 14.1, we have $S^0 \neq V'$.*

Theorem 16. *If M is an m-dimensional subspace of an n-dimensional vector space V, then M^0 is an $(n - m)$-dimensional subspace of V'.*

Proof. Let $y, y' \in M^0$, then $[x, y] = 0 = [x, y']$ $\forall x \in M$. For any scalars α, β, we see that $[x, \alpha y + \beta y'] = \alpha[x, y] + \beta[x, y'] = 0$, so $\alpha y + \beta y' \in M^0$. Thus M^0 is a subspace of V'.

Now consider a basis $X = \{x_1, \cdots, x_n\}$ for V such that first m elements of X form a basis for M which is possible by Corollary 7.1 (Section 1.2). Let $X' = \{y_1, \cdots, y_n\}$ be the dual basis for V'. Let N be the subspace spanned by the last $n - m$ vectors of X'. We shall prove that $N = M^0$.

Any vector $x \in M$, can be written as $x = \sum_{i=1}^{m} \xi_i x_i$, then notice that for any $j = m + 1, \cdots, n$ we have $[x, y_j] = \sum_{i=1}^{m} \xi_i[x_i, y_j] = 0$. Thus, $N \subseteq M^0$.

Now consider any element y of M^0, then $y = \sum_{j=1}^{n} \zeta_j y_j$. But $y \in M^0$, so for any $x_i \in M$ we have

$$0 = [x_i, y] = \left[x_i, \sum_{j=1}^{n} \zeta_j y_j\right] = \sum_{j=1}^{n} \zeta_j[x_i, y_j] = \zeta_i,$$

in other words, for any element $y = \sum_{j=1}^{n} \zeta_j y_j$ in M^0, we have $\zeta_j = 0$ $\forall j, 1 \leq j \leq m$. So $M^0 \subseteq N$. Therefore, $M^0 = N$ and it is a $(n - m)$ dimensional subspace of V'. $\square$

Corollary 16.1. *If M is a subspace in a finite-dimensional vector space V, then $M^{00}(= (M^0)^0) = M$.*

Proof. Notice that here we adopted the notation established in Note 7 that identifies V'' and V. By applying the Definition 14 on M^0, we see that M^{00} is the set of all vectors x such that $[x, y] = 0$ $\forall y \in M^0$ and this x does not have to belong to M. Now applying the same definition on M, we have $\forall x \in M, [x, y] = 0$ $\forall y \in M^0$. Thus $M \subseteq M^{00}$.

Now we show that the converse also holds. By the Theorem 16, if M is m-dimensional subspace of V, then M^0 is $(n - m)$-dimensional subspace of V'. Now again by $(n - m)$-dimensionality of M^0, the dimension of M^{00} will be $n - (n - m) = m$, thus $M^{00} = M$. $\square$

Theorem 17. *If M and N are subspaces of a vector space V, and if $V = M \oplus N$, then M' is isomorphic to N^0 and N' to M^0 and $V' = M^0 \oplus N^0$.*

Proof. **{Change the notation used}**

To simplify the notation we shall use, throughout this proof, x, x', and x^0 for elements of M, M', and M^0, respectively, and we reserve, similarly, the letters y for N and z for V. (This notation is not meant to suggest that there is any particular relation between, say, the vectors x in M and the vectors x' in M'.)

We proceed to prove that V' is the direct sum of M^0 and N^0. Since $V = M \oplus N$, every vector in V can be written as $z = x + y$ in a one and only one way (by Theorem 10). If z' belongs to both M^0 and N^0, i.e, $z'(x) = 0 = z'(y)$, $\forall x, y$, then $z'(z) = z'(x + y) = z'(x) + z'(y) = 0 \ \forall z$. So if $z' \in M^0$ and N^0, then z' is the zero linear functional, thus $M^0 \cap N^0 = \{0\} \subset V'$. Let z' be any element in V' and if $z = x + y$, then $z'(x + y) = z'(x) + z'(y)$. Now we define $x^0(z) = z'(y)$ and $y^0(z) = z'(x)$ so that any vector in V' is written as $z' = x^0 + y^0$. Then $\forall x, y$, we see that $x^0(x) = 0 = y^0(y)$ which means that $x^0 \in M^0$ and $y^0 \in N^0$. This shows that $V' = M^0 + N^0$. Therefore, $V' = M^0 \oplus N^0$.

Now we establish the isomorphisms. Consider the map between M^0 and N' $x^0 \mapsto y'$ defined by $y'(y) = x^0(y)$, i.e, $[y, y'] = [y, x^0]$. Consider an element $\alpha x_1^0 + \beta x_2^0$ such that $x_1^0 \mapsto y_1'$ and $x_2^0 \mapsto y_2'$. Then, we have

$$[y, \alpha x_1^0 + \beta x_2^0] = \alpha[y, x_1^0] + \beta[y, x_2^0] = \alpha[y, y_1'] + \beta[y, y_2'] = [y, \alpha y_1' + \beta y_2'].$$

So, $\alpha x_1^0 + \beta x_2^0 \mapsto \alpha y_1' + \beta y_2'$, thus this map is linear. Now suppose $y_1' = y_2'$, i.e, $[y, y_1'] = [y, y_2'] \ \forall y$, then we have $[y, x_1^0] = [y, x_2^0] \implies [y, x_1^0 - x_2^0] = 0 \ \forall y$. Then, by Corollary 14.1, we have $x_1 = x_2$, therefore the map is one-to-one. Now comparing the dimensions of each of the vector spaces we can directly conclude that M^0 and N' are isomorphic. By the symmetry of the argument we can also conclude that N^0 and M' are isomorphic. $\square$

1.6   Quotient Spaces

Definition 15. *Let M be a subspace of a vector space V and x is any vector in V. Then, by $x + M$ we denote the following set:*

$$x + M = \{x + m \mid \forall m \in M\}.$$

*Each set of the form $x + M$ is called **coset** of M in V.*

Remark 6. *Notice that if $x \in M$, then $x + M = M$.*

Remark 7. *Let $x \neq y$ be any two vectors in V. Then $x + M = y + M \Leftrightarrow x - y \in M$. In other words, $x + M = y + M$ doesn't necessarily imply that $x = y$. With regard to this fact, from now on we drop the element x and simply refer a coset of M as a set $\mathcal{H}$, then a set $\mathcal{H}$ is a coset of M if there exists atleast one $x \in V$ such that $\mathcal{H} = x + M$.*

Definition 16. *For any two cosets of M, $\mathcal{H}$ and $\mathcal{K}$, we define addition of cosets as the following:*
$$\mathcal{H} + \mathcal{K} = \{u + v \mid \forall u \in \mathcal{H}, v \in \mathcal{K}\}.$$

For every coset $\mathcal{H}$ of M, we define $-\mathcal{H}$ as the following:

$$-\mathcal{H} = \{-u \mid \forall\ u \in \mathcal{H}\} = -x + M$$

and for any scalar $\alpha \neq 0$, we define the scalar multiplication as follows:

$$\alpha \mathcal{H} = \{\alpha u \mid \forall u \in M\}$$

and for $\alpha = 0$, we define $0 \cdot \mathcal{H} = \mathcal{M}$.

Lemma 18 (Coset Operations)**.** *Let M be a subspace of V. Then,*

i) *For any cosets $\mathcal{H}$ and $\mathcal{K}$ of M, $\mathcal{H} + \mathcal{K}$ is also a coset of M.*

ii) *Coset addition is commutative and associative.*

iii) *The coset $\mathcal{M}$ (i.e, $0+M$) is the only coset with the property that $\mathcal{H}+\mathcal{M} = \mathcal{H}$ for every coset $\mathcal{H}$.*

iv) *The coset $-\mathcal{H}$ is the only coset with the property that $\mathcal{H} + (-\mathcal{H}) = \mathcal{M}$.*

v) *For any scalar α, $\alpha \mathcal{H}$ is also a coset.*

vi) *Scalar multiplication of cosets is associative and it is distributive over scalar and vector addition.*

Proof. i) Suppose $\mathcal{H}, \mathcal{K}$ are any two cosets of M, then from the Definition 16 we have $\mathcal{H} + \mathcal{K} = \{u + v \mid \forall u \in \mathcal{H}, v \in \mathcal{K}\}$. But $u = x + z$ and $y + z$ for some $x, y \in V$ and $z \in M$. Then every element of $\mathcal{H} + \mathcal{K}$ $u + v = x' + z', x' = x + y \in V, z' = 2z \in M$, so $\mathcal{H} + \mathcal{K} = x' + M$, hence it is a coset of M.

ii) Commutativity and associativity are trivially satisfied due to i) and from the commutative and associative laws of vector addition.

iii) Let $\mathcal{H} = x + M$ and $\mathcal{K} = y + M$ and suppose that $\mathcal{H} + \mathcal{K} = \mathcal{H}$. Then $(x + y) + M = x + M$, which implies that $x + y \in x + M$, i.e, $x + y = x + u$ for some $u \in M$, then we get $y \in M$. So $\mathcal{H} + \mathcal{K} = \mathcal{H} \Leftrightarrow \mathcal{K} = \mathcal{M}$.

iv) Suppose that for some $\mathcal{H} \neq \mathcal{M}$, we have $\mathcal{H} + \mathcal{K} = \mathcal{M}$, then $(x+y)+M = M$, implies $x + y \in M$. Since $x \notin M$, then $x + y \in M \Leftrightarrow y = -x$. Thus $\mathcal{K} = -x + M = -\mathcal{H}$.

v) If $\mathcal{H} = x + M$, then for every $u \in M, \alpha(x + u) \in \alpha \mathcal{H}$, then $\alpha x + u' \in \alpha \mathcal{H}$ where $u' = \alpha u \in M$, so $\alpha \mathcal{H} = (\alpha x) + M$.

vi) These properties are trivially satisfied due to v) and the associative and it is distributive laws of scalar multiplication over scalar and vector addition. $\square$

Theorem 19. *The set of all cosets is a vector space with respect to the linear operations defined in Lemma 18. This vector space is called the **quotient space** of V modulo M; it is denoted by V/M.*

Proof. From Lemma 18 and Definition 2. $\square$

Theorem 20. *Let M and N be two subspaces of V such that $M \oplus N = V$. Then the correspondence that assigns to each vector y in N the coset $y + M$ is an isomorphism between N and V/M.*

Proof. First we show that the map is one-to-one. Let $y_1, y_2 \in N$ and suppose that $y_1 + M = y_2 + M$. Then by Remark 7, we see that $y_1 - y_2 \in M$. But M and N are complmentary spaces, so $y_1 = y_2$. Thus the map is one-to-one.

Now to show that the map is onto. Let $z + M$ be any arbitrary coset of M for some $z \in V$. Since V is the direct sum of M and N, we can decompose z as

$x + y, x \in M, y \in N$, then $z + M = (x + y) + M = y + (x + M) = y + M$, since $x \in M$. So for every coset of M, we have corresponding element to it in N.

For any scalars α_1, α_2 and $y_1, y_2 \in N$, consider

$$(\alpha_1 y_1 + \alpha_2 y_2) + M = (\alpha_1 y_1 + \alpha_2 y_2) + (\alpha_1 + \alpha_2)M = \alpha_1(y_1 + M) + \alpha_2(y_2 + M).$$

This the correspondence is an isomorphism. $\qquad\square$

Theorem 21. *If M is an m-dimensional subspace of an n-dimensional vector space V, then V/M has dimension $n - m$.*

Proof. By Theorem 12, we can find a subspace N such that $M \oplus N = V$, and $dim(N) = n - m$. Then by Theorem 20, we have an isomorphism between N and V/M. Thus $dim(V/M) = n - m$. $\qquad\square$

References

[1] Halmos, P., 1955. Finite Dimensional Vector Spaces. Princeton University Press.

[2] Cherney, D., Denton, T., Thomas, R. and Waldron, A., 2016. Linear Algebra. [online] Available at: `https://www.math.ucdavis.edu/~linear/`.