Note 1.7.8. Let U and W be subspaces over a vector space V. Then $U \cap W$ is also a subspace of V.

Moreover, $U \cap W$ is the largest subspace of V which is contained in both U and W [Why?]. Thus $U \cap W$ acts like a greatest lower bound for U and W within the set of subspaces of V, i.e.,

$$U \cap W = \text{glb}\{U, W\} \text{ in } \{X \mid X \preceq V\}.$$

What about a least upper bound for U and W in the set of subspaces of V?

$$\text{lub}\{U, W\} \text{ in } \{X \mid X \preceq V\} = ?$$

Is $U \cup W$ this least upper bound?

Definition 1.7.9. Let $S_1, S_2, \ldots, S_k$ be non-empty subsets of a vector space. Then the *sum* of the subsets $S_1, S_2, \ldots, S_k$, denoted by $S_1 + S_2 + \cdots + S_k$ or $\sum_{i=1}^{k} S_i$, is defined to be

$$S_1 + S_2 + \cdots + S_k := \{x_1 + x_2 + \cdots + x_k \mid x_i \in S_i \text{ for all } i\}.$$

Proposition 1.7.10. *Let V be a vector space over a field and $W_1, W_2, \ldots, W_k \preceq V$. Then*

(i) the sum $W_1 + W_2 + \cdots + W_k$ is a subspace of V which contains each of the subspace W_i;

(ii) $W_1 + W_2 + \cdots + W_k = \langle W_1 \cup W_2 \cup \cdots \cup W_k \rangle$.

1.8 Linearly Independence and Bases

Definition 1.8.1. Let V be a vector space over a field F and $v_1, v_2, \ldots, v_n \in V$. For any $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, the element $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \in V$ is called a *linear combination of* $v_1, v_2, \ldots, v_n$.

If $\alpha_i = 0$ for all i, it is called the *trivial linear combination of* $v_1, v_2, \ldots, v_n$; if $\alpha_i \neq 0$ for at least one i, then it is called a *non-trivial linear combination of* $v_1, v_2, \ldots, v_n$.

Definition 1.8.2. Let V be a vector space over a field F and $S \subseteq V$. We call the set S *linearly dependent* (or simply, *dependent*) if there exist **finite** distinct vectors $x_1, x_2, \ldots, x_n \in S$ and **finite** scalars $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, not all of which are 0, such that

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0.$$

We call the set S *linearly independent* if it is not linearly dependent.

Remark 1.8.3. We may rephrase the above definition as follows:

S is linearly dependent if and only if there exists a finite set $\{x_1, x_2, \ldots, x_n\}$ of distinct elements of S such that at least one non-trivial linear combination of $x_1, x_2, \ldots, x_n$ equals 0.

S is linearly independent if and only if for all finite sets $\{x_1, x_2, \ldots, x_n\}$ of distinct elements of S and for all $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, a linear combination $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ is always trivial.

S is linearly independent if and only if for all distinct **finite** elements $x_1, x_2, \ldots, x_n \in S$ and for all **finite** scalars $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, if $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$, then $\alpha_i = 0$ for all i.

If the set S contains only finitely many vectors $x_1, x_2, \ldots, x_n$, we sometimes say that $x_1, x_2, \ldots, x_n$ are dependent (or independent) instead of saying S is dependent (or independent).

Note 1.8.4.

(i) Any set which contains a linearly dependent set is linearly **dependent/independent**.

(ii) Any subset of a linearly independent set is linearly **dependent/independent**.

(iii) Any set which contains 0 is linearly **dependent/independent**.

(iv) If $S = \{x_1, x_2, \ldots, x_n\}$ is a finite set, then S is linearly independent if and only if for all $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, if $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n = 0$, then $\alpha_i = 0$ for all i. It is not necessary to consider all finite subsets of S. Prove it!

Example 1.8.5.

(i) Let $S = \{2x^2 + x + 4, 3x^2 - x - 1, x + 3\} \subseteq \mathbb{Z}_5[x]$. Is S linearly dependent or independent?

(ii) Let $S = \{2x^2 + x + 4, x^2 + x + 3, x + 2\} \subseteq \mathbb{Z}_5[x]$. Is S linearly dependent or independent?

(iii) Let $S = \{x, \sin x, \cos x\} \subseteq \mathbb{R}^{\mathbb{R}}$. Is S linearly dependent or independent?

Lemma 1.8.6. *Let V be a vector space over a field F and $S \subseteq V$ such that S is linearly independent. Suppose that $x_1, x_2, \ldots, x_n$ are distinct elements of S and $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in F$ are such that there exists i with $\alpha_i \neq \beta_i$. Then*

$$\alpha_1 x_1 + \cdots + \alpha_n x_n \neq \beta_1 x_1 + \cdots + \beta_n x_n.$$

If S is a linearly independent subset of a vector space V, then Lemma 1.8.6 says that every $v \in \langle S \rangle$ is a unique linear combination of elements of S in 'some sense', e.g., ignore the case $\alpha_1 x_1 + \cdots + \alpha_n x_n = \alpha_1 x_1 + \cdots + \alpha_n x_n + 0x_{n+1} + 0x_{n+2} + \cdots$. In particular, if $\langle S \rangle = V$, then every element of V can be expressed as a unique linear combination of elements of S.

Definition 1.8.7. Let V be a vector space over a field and $S \subseteq V$. We call S a *basis* of V if

(i) S spans V, i.e., $\langle S \rangle = V$, and

(ii) S is linearly independent.

Lemma 1.8.8. *Let V be a vector space over a field F and S a basis of V. Then for each $v \in V$, if $v \neq 0$, then there exist a unique set $\{x_1, x_2, \ldots, x_n\}$ of distinct elements of S and a unique set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of non-zero elements of F such that*

$$v = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

Proof. Let $v \in V\backslash\{0\}$.
Existence: Since $V = \langle S \rangle$, there exist $z_1, z_2, \ldots, z_k \in S$ and $\gamma_1, \gamma_2, \ldots, \gamma_k \in F$ such that $v = \gamma_1 z_1 + \gamma_2 z_2 + \cdots + \gamma_k z_k$. Note that $z_1, z_2, \ldots, z_k$ may repeat or some of $\gamma_1, \gamma_2, \ldots, \gamma_k$ may be zero. If $z_i = z_j$ for some $i < j$, then we rewrite v as

$$v = \gamma_1 z_1 + \cdots + \gamma_{i-1} z_{i-1} + (\gamma_i + \gamma_j) z_i + \gamma_{i+1} z_{i+1} + \cdots + \gamma_{j-1} z_{j-1} + \gamma_{j+1} z_{j+1} + \cdots + \gamma_k z_k.$$

This shows that v is a linear combination of $z_1, z_2, \ldots, z_{j-1}, z_{j+1}, \ldots, z_k$. If these are distinct, we are done for the existence of distinct elements of S. If not, we repeat this process as often as necessary, until we obtain distinct $y_1, \ldots, y_m \in S$ and scalars $\beta_1, \ldots, \beta_m \in F$ such that $v = \beta_1 y_1 + \cdots + \beta_m y_m$.

Now, if some $\beta_i = 0$, then

$$v = \beta_1 y_1 + \cdots + \beta_{i-1} y_{i-1} + \beta_{i+1} y_{i+1} + \cdots + \beta_m y_m,$$

a linear combination of $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_m$. If necessary, we may repeat this process until we obtain **distinct** $x_1, x_2, \ldots, x_n \in S$ and non-zero scalars $\alpha_1, \alpha_2, \ldots, \alpha_n$ such that

$$v = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

Uniqueness: Suppose that $x'_1, \ldots, x'_m$ are distinct elements of S and $\alpha'_1, \ldots, \alpha'_m$ are non-zero scalars such that

$$v = \alpha'_1 x'_1 + \cdots + \alpha'_m x'_m.$$

We must show that $m = n$, and after re-numbering if necessary,

$$x_i = x'_i \quad \text{and} \quad \alpha_i = \alpha'_i \quad \text{for all } i = 1, 2, \ldots, n.$$

First, we re-number $x'_1, \ldots, x'_m$ if necessary so that

$$x'_i = x_i \text{ for all } i = 1, \ldots, k \text{ and } \{x_{k+1}, \ldots, x_n\} \cap \{x'_{k+1}, \ldots, x'_m\} = \emptyset.$$

Let $w_i = x_i$ for all $i = 1, \ldots, n$ and $w_{n+i} = x'_{k+i}$ for all $i = 1, \ldots, m-k$, i.e.,

$$\begin{array}{ccccccccc} x_1, & \ldots, & x_k, & x_{k+1}, & \ldots, & x_n, & & & \\ x'_1, & \ldots, & x'_k, & & & & x'_{k+1}, & \ldots, & x'_m \\ w_1, & \ldots, & w_k, & w_{k+1}, & \ldots, & w_n, & w_{n+1}, & \ldots, & w_{n+(m-k)} \end{array}$$

Now, we have

$$\{w_1, \ldots, w_{n+m-k}\} = \{x_1, \ldots, x_n\} \cup \{x'_1, \ldots, x'_m\}$$

and the elements $w_1, \ldots, w_{n+m-k} \in S$ are all distinct.

Next, we would like to apply Lemma 1.8.6, so we will write v as two ways of linear combinations of $w_1, \ldots, w_{n+m-k}$. Next, define

$$\beta_i = \begin{cases} \alpha_i, & \text{if } 1 \le i \le n, \\ 0, & \text{if } n+1 \le i \le n+m-k, \end{cases} \qquad \text{and} \qquad \beta'_i = \begin{cases} \alpha'_i, & \text{if } 1 \le i \le k, \\ 0, & \text{if } k+1 \le i \le n, \\ \alpha'_{i+k-n}, & \text{if } n+1 \le i \le n+m-k, \end{cases}$$

i.e.,

$$\begin{array}{lccccccccc}
\beta_i \Longrightarrow & \alpha_1, & \ldots, & \alpha_k, & \alpha_{k+1}, & \ldots, & \alpha_n, & 0, & \ldots, & 0 \\
& x_1, & \ldots, & x_k, & x_{k+1}, & \ldots, & x_n, & & & \\
\beta_i' \Longrightarrow & \alpha_1', & \ldots, & \alpha_k', & 0, & \ldots, & 0, & \alpha_{k+1}', & \ldots, & \alpha_m' \\
& x_1', & \ldots, & x_k', & & & & x_{k+1}', & \ldots, & x_m' \\
& w_1, & \ldots, & w_k, & w_{k+1}, & \ldots, & w_n, & w_{n+1}, & \ldots, & w_{n+(m-k)}
\end{array}$$

Now, we obtain that

$$\beta_1 w_1 + \cdots + \beta_{n+m-k} w_{n+m-k} = v = \beta_1' w_1 + \cdots + \beta_{n+m-k}' w_{n+m-k}.$$

Note also that S is a basis of V, and hence is linearly independent. By the contrapositive of Lemma 1.8.6, we must have $\beta_i = \beta_i'$ for all $i = 1, 2, \ldots, n+m-k$. Suppose that $k < n$. Then $\beta_{k+1}' = 0$ while $\beta_{k+1} = \alpha_{k+1} \neq 0$, a contradiction. Thus $k = n$. Suppose that $n < m$.Then $\beta_{n+1} = 0$ but $\beta_{n+1}' = \alpha_{k+1}' \neq 0$, a contradiction. Hence we must have $m = n$.

This shows that $m = n = k$. But recall that $x_i' = x_i$ for all $i = 1, 2, \ldots, k$, so in fact $x_i' = x_i$ for all $i = 1, 2, \ldots, n$. Finally, we also obtain that $\alpha_i' = \beta_i' = \beta_i = \alpha_i$ for all $i = 1, 2, \ldots, n$. □

Note 1.8.9. Lemma 1.8.8 says that

If S is a basis of a vector space V, then every element of V can be written as a unique linear combination of elements of S.

Questions:

(i) Does every vector space have a basis?

(ii) Can a vector space have more than one basis? If so, do these bases have anything in common?

Lemma 1.8.10. *Let V be a vector space over a field and $S \subseteq V$ such that S is maximal linearly independent, i.e., S is linearly independent and for any linearly independent $S' \subseteq V$ if $S \subseteq S'$, then $S = S'$. Then S is a basis of V.*

Definition 1.8.11. A *partially ordered set (POSET)* is a set P together with a binary relation $\leq$ on P satisfying the following axioms:

(i) Reflexive: $\forall\, x \in P \;\; x \leq x$

(ii) Transitive: $\forall\, x, y, z \in P \;\; x \leq y$ and $y \leq z \Longrightarrow x \leq z$

(iii) Anti-Symmetric: $\forall\, x, y \in P \;\; x \leq y$ and $y \leq x \Longrightarrow x = y$.

A *chain* in P is a subset $C \subseteq P$ such that $\forall\, x, y \in C \;\; x \leq y$ or $y \leq x$.

If S is any subset of P, an *upper bound of S (in P)* is an element $u \in P$ such that $x \leq u$ for all $x \in S$.

A *maximal element of P* is an element $m \in P$ such that $\forall\, x \in P \;\; m \leq x \Longrightarrow m = x$.

Lemma 1.8.12. Zorn's Lemma

Let P be a non-empty POSET. If every chain in P has an upper bound in P, then P has a maximal element.

Note that Zorn's Lemma is equivalent to the Axiom of Choice.

Theorem 1.8.13. *Let V be a vector space over a field and $S \subseteq V$ linearly independent. Then there exists a basis B of V such that $S \subseteq B$.*

In particular, V has at least one basis.

Remark 1.8.14. Theorem 1.8.13 can be rephrased as the followings:

Every linearly independent subset of a vector space can be extended to a basis.

Lemma 1.8.15. *Let V be a vector space and $S = \{x_1, x_2, \ldots, x_n\}$ be a linearly independent subset of distinct elements of V. Also, let $T \subseteq V$ be such that T spans V, i.e., $\langle T \rangle = V$. Then for each $i \in \{1, 2, \ldots, n\}$ there exists $y_i \in T$ such that $\{x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_n\}$ with n distinct elements is linearly independent.*

Theorem 1.8.16. *Let V be a vector space. If V has an infinite basis, then every basis of V is infinite, and they all have the same cardinality.*

Theorem 1.8.17. *Let V be a vector space. If V has a finite basis, then every basis of V is finite, and they all have the same cardinality.*

Rewrite the above theorem to be

Theorem 1.8.17* Let V be a vector space. If V has a finite basis of order n, then

(i) every basis of V is finite of order not more than n, and

(ii) they all have the same cardinality n.

Definition 1.8.18. Let V be a vector space. The *dimension* of V, denoted by $\dim V$, is the cardinality of any basis of V. If $\dim V$ is a finite cardinal number, we say that V is the *finite-dimensional*; otherwise, we say that V is *infinite-dimensional*. In particular, if $\dim V = k$, where $k \in \mathbb{N}$, we say that V is *k-dimensional*.

Corollary 1.8.19. *Let V be an n-dimensional vector space. Then*

(i) any subset of V which contains more than n vectors is linearly dependent; and

(ii) no subset of V which contains less than n vectors can span V.

Note 1.8.20. If V is any vector space, then the zero subspace of V is spanned by the zero vector 0, but $\{0\}$ is a linearly dependent set so that it cannot be a basis of V. However, we can show that $\emptyset$ spans $\{0\}$ and $\emptyset$ is linearly independent so that $\emptyset$ is a basis of $\{0\}$. Therefore, $\dim\{0\} = 0$.

Lemma 1.8.21. *Let S be a linearly independent subset of a vector space V. Suppose that v is a vector in V which is not in the subspace spanned by S. Then $S \cup \{v\}$ is linearly independent.*

Theorem 1.8.22. *Let V be a vector space and W a subspace of V. Then $\dim W \le \dim V$. Moreover, if V is finite-dimensional and $\dim W = \dim V$, then $W = V$.*

Corollary 1.8.23. *Let V be a finite-dimensional vector space and B a linearly independent subset of V. If* $\operatorname{card} B = \dim V$*, then B is a basis of V.*

Theorem 1.8.24. *Let S be a subset of a vector space V such that S spans V. Then there exists a basis B of V such that $B \subseteq S$.*

Corollary 1.8.25. *Let S be a subset of a finite-dimensional vector space V such that S spans V. If* $\operatorname{card} S = \dim V$*, then S is a basis of V.*

Example 1.8.26.

(i) Let F be a field, $n \in \mathbb{N}$ and $i \in \{1, 2, \ldots, n\}$. The ith standard vector in F^n is the vector e_i that has 0s in all coordinate positions except the ith, where it has a 1. Thus

$$e_i = (0, \ldots, 0, \overbrace{\ 1\ }^{\text{the } i\text{th}}, 0, \ldots, 0).$$

The set $\{e_1, e_2, \ldots, e_n\}$ is called the *standard basis* of F^n.

(ii) Let A be an invertible $n \times n$ matrix with entries in the field F. Then $A_1, A_2, \ldots, A_n$, the columns of A, form a basis for the space of column matrices, $M_{n\times 1}(F)$.

(iii) (An example of an infinite basis) Let F be a field with $\operatorname{char} F = 0$ and $V = F[x] = F^F$. Recall that

$$V = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N} \cup \{0\}, a_i \in F \text{ for all } i\}.$$

Define $f_k(x) = x^k$ for all $k = 0, 1, 2, \ldots$. The infinite set $\{f_0, f_1, f_2, \ldots\}$ is a basis of V.