Vector Space Theory

Jason Sass

June 6, 2025

Vector Spaces

Theorem 1. ***alternate definition of a vector space***

Let V be a set.

Define binary operation $+ : V \times V \to V$ by $\vec{v} + \vec{w} \in V$ for all $\vec{v}, \vec{w} \in V$. ***(vector addition)***

Let F be a field.

Define function $\cdot : F \times V \to V$ by $\lambda\vec{v} \in V$ for all $\lambda \in F$ and for all $\vec{v} \in V$. ***(scalar multiplication)***

Then $(V, +, \cdot)$ is a ***vector space over a field*** *F iff*

1. $(V, +)$ is an abelian group.

2. Associativity of scalar multiplication with field multiplication
$\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$ for all $\vec{v} \in V$ and for all $\alpha, \beta \in F$.

3. Left distributive law of scalar multiplication over vector addition
$\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$ for all $\vec{v}, \vec{w} \in V$ and for all $\lambda \in F$.

4. Right distributive law of scalar multiplication over scalar addition
$(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$ for all $\vec{v} \in V$ and for all $\alpha, \beta \in F$.

5. $1 \in F$ is a multiplicative identity for scalar multiplication.
$1 \cdot \vec{v} = \vec{v}$ for all $\vec{v} \in V$.

Proof. Suppose $(V, +, \cdot)$ is a vector space over F.

Then vector addition is associative and commutative, and there exists a right additive identity in V, and every element of V has a right additive inverse, and associativity of scalar multiplication with field multiplication holds, and the left distributive law of scalar multiplication over vector addition holds, and the right distributive law of scalar multiplication over scalar addition holds, and $1 \in F$ is a multiplicative identity for scalar multiplication.

Since vector addition is a binary operation on V, and vector addition is associative, and there is a right additive identity in V, and every element of V has a right additive inverse, then $(V, +)$ is a group, by the right-sided definition of group.

Since $(V, +)$ is a group, and vector addition is commutative, then $(V, +)$ is an abelian group.

Therefore, $(V, +)$ is an abelian group, and associativity of scalar multiplication with field multiplication holds, and the left distributive law of scalar multiplication over vector addition holds, and the right distributive law of scalar multiplication over scalar addition holds, and $1 \in F$ is a multiplicative identity for scalar multiplication, as desired.

Conversely, suppose $(V, +)$ is an abelian group, and associativity of scalar multiplication with field multiplication holds, and the left distributive law of scalar multiplication over vector addition holds, and the right distributive law of scalar multiplication over scalar addition holds, and $1 \in F$ is a multiplicative identity for scalar multiplication.

Since $(V, +)$ is an abelian group, then vector addition is associative and commutative, and there is an additive identity in V, and every element of V has an additive inverse.

Since there is an additive identity in V, then there exists $\vec{0} \in V$ such that $\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}$ for all $\vec{v} \in V$, so there exists $\vec{0} \in V$ such that $\vec{v} + \vec{0} = \vec{v}$ for all $\vec{v} \in V$.

Hence, $\vec{0} \in V$ is a right additive identity.

Since every element of V has an additive inverse, then for every $\vec{v} \in V$, there exists $-\vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = -\vec{v} + \vec{v} = \vec{0}$, so for every $\vec{v} \in V$, there exists $-\vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = \vec{0}$.

Hence, every element of V has a right additive inverse.

Since vector addition is a binary operation on V defined by $+ : V \times V \to V$ $\vec{v} + \vec{w} \in V$ for all $\vec{v}, \vec{w} \in V$, and scalar multiplication is a function $F \times V \to V$ defined by $\lambda\vec{v} \in V$ for all $\lambda \in F$ and for all $\vec{v} \in V$, and vector addition is associative and commutative, and $\vec{0} \in V$ is a right additive identity, and every element of V has a right additive inverse, and associativity of scalar multiplication with field multiplication holds, and the left distributive law of scalar multiplication over vector addition holds, and the right distributive law of scalar multiplication over scalar addition holds, and $1 \in F$ is a multiplicative identity for scalar multiplication, then $(V, +, \cdot)$ is a vector space over F, as desired. □

Theorem 2. ***basic properties of vector spaces***

Let $(V, +, \cdot)$ be a vector space over a field F.

1. Any scalar times the zero vector is the zero vector.

$\lambda\vec{0} = \vec{0}$ for all $\lambda \in F$.

2. Zero times any vector is the zero vector.

$0\vec{v} = \vec{0}$ for all $\vec{v} \in V$.

3. The scalar product is zero iff the scalar is zero or the vector is zero.

$\lambda\vec{v} = \vec{0}$ iff $\lambda = 0$ or $\vec{v} = \vec{0}$, for all $\vec{v} \in V$ and for all $\lambda \in F$.

4. Negative 1 times any vector is the additive inverse of the vector.

$(-1)\vec{v} = -\vec{v}$ for all $\vec{v} \in V$.

Proof. We prove 1.

Let $\lambda \in F$.

Since $\vec{0} \in V$ and $\vec{0}$ is additive identity, then $\vec{0} + \vec{0} = \vec{0}$.
Thus, $\lambda\vec{0} + \lambda\vec{0} = \lambda(\vec{0} + \vec{0}) = \lambda\vec{0}$, so $\lambda\vec{0} + \lambda\vec{0} = \lambda\vec{0}$.
We add the additive inverse of $\lambda\vec{0}$ to both sides of the equation.
Observe that

$$\begin{aligned}(\lambda\vec{0} + \lambda\vec{0}) + [-(\lambda\vec{0})] &= \lambda\vec{0} + [-(\lambda\vec{0})] \\ \lambda\vec{0} + [\lambda\vec{0} + -(\lambda\vec{0})] &= \vec{0} \\ \lambda\vec{0} + \vec{0} &= \vec{0} \\ \lambda\vec{0} &= \vec{0}.\end{aligned}$$

Therefore, $\lambda\vec{0} = \vec{0}$, as desired. □

Proof. We prove 2.
Let $\vec{v} \in V$.
Since $0\vec{v} + 0\vec{v} = (0 + 0)\vec{v} = 0\vec{v}$, then $0\vec{v} + 0\vec{v} = 0\vec{v}$.
We add the additive inverse of $0\vec{v}$ to both sides of the equation.
Observe that

$$\begin{aligned}(0\vec{v} + 0\vec{v}) + [-(0\vec{v})] &= 0\vec{v} + [-(0\vec{v})] \\ 0\vec{v} + [0\vec{v} + -(0\vec{v})] &= \vec{0} \\ 0\vec{v} + \vec{0} &= \vec{0} \\ 0\vec{v} &= \vec{0}.\end{aligned}$$

Therefore, $0\vec{v} = \vec{0}$, as desired. □

Proof. We prove 3.
Let $\vec{v} \in V$ and $\lambda \in F$.
Suppose $\lambda = 0$ or $\vec{v} = \vec{0}$.
If $\lambda = 0$, then $\lambda\vec{v} = 0\vec{v} = \vec{0}$.
If $\vec{v} = \vec{0}$, then $\lambda\vec{v} = \lambda\vec{0} = \vec{0}$.

Conversely, suppose $\lambda\vec{v} = \vec{0}$.
To prove $\lambda = 0$ or $\vec{v} = \vec{0}$, assume $\lambda \neq 0$.
We must prove $\vec{v} = \vec{0}$.
Since F is a field and $\lambda \in F$ and $\lambda \neq 0$, then λ has a multiplicative inverse in F.
Thus, there exists $\lambda^{-1} \in F$ such that $\lambda \cdot \lambda^{-1} = \lambda^{-1} \cdot \lambda = 1$.
Observe that

$$\begin{aligned}\vec{v} &= 1 \cdot \vec{v} \\ &= (\lambda^{-1} \cdot \lambda)\vec{v} \\ &= (\lambda^{-1})(\lambda\vec{v}) \\ &= (\lambda^{-1})\vec{0} \\ &= \vec{0}.\end{aligned}$$

Therefore, $\vec{v} = \vec{0}$, as desired. □

Proof. We prove 4.

Let $\vec{v} \in V$.

Observe that

$$\begin{aligned} \vec{0} &= 0 \cdot \vec{v} \\ &= (-1+1)\vec{v} \\ &= (-1)\vec{v} + 1\vec{v} \\ &= (-1)\vec{v} + \vec{v}. \end{aligned}$$

Hence, $\vec{0} = (-1)\vec{v} + \vec{v}$.

We add the additive inverse of $\vec{v}$ to both sides of the equation.

Observe that

$$\begin{aligned} \vec{0} + (-\vec{v}) &= [(-1)\vec{v} + \vec{v}] + (-\vec{v}) \\ -\vec{v} &= (-1)\vec{v} + [\vec{v} + (-\vec{v})] \\ -\vec{v} &= (-1)\vec{v} + \vec{0} \\ -\vec{v} &= (-1)\vec{v}. \end{aligned}$$

Therefore, $(-1)\vec{v} = -\vec{v}$, as desired. □

Linear subspaces

Theorem 3. ***Two-Step Subspace Test***

Let $(V, +, \cdot)$ be a vector space over a field F.
Let W be a nonempty subset of V.
Then W is a subspace of V iff
1. W is closed under vector addition.
$\vec{v} + \vec{w} \in W$ for all $\vec{v}, \vec{w} \in W$ (Closure under vector addition)
2. W is closed under scalar multiplication.
$\lambda\vec{v} \in W$ for all $\vec{v} \in W, \lambda \in F$ (Closure under scalar multiplication)

Proof. Suppose W is closed under vector addition and scalar multiplication.

Since $(V, +, \cdot)$ is a vector space over F, then V is closed under vector addition, and vector addition over V is associative and commutative, and $\vec{0} \in V$ is additive identity, and every vector in V has an additive inverse in V, and V is closed under scalar multiplication, and associativity of scalar multiplication with field multiplication holds, and the left distributive law of scalar multiplication over vector addition holds, and the right distributive law of scalar multiplication over scalar addition holds, and $1 \in F$ is a multiplicative identity for scalar multiplication.

We prove $(W, +, \cdot)$ is a vector space.

Let $\vec{u}, \vec{v}, \vec{w} \in W$.

Since $\vec{u}, \vec{v}, \vec{w} \in W$ and $W \subset V$, then $\vec{u}, \vec{v}, \vec{w} \in V$.

Since vector addition over V is associative, then $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$.

Therefore, $(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$ for all $\vec{u}, \vec{v}, \vec{w} \in W$, so vector addition over W is associative.

Let $\vec{v}, \vec{w} \in W$.

Since $\vec{v}, \vec{w} \in W$ and $W \subset V$, then $\vec{v}, \vec{w} \in V$.

Since vector addition over V is commutative, then $\vec{v} + \vec{w} = \vec{w} + \vec{v}$.

Therefore, $\vec{v} + \vec{w} = \vec{w} + \vec{v}$ for all $\vec{v}, \vec{w} \in W$, so vector addition over W is commutative.

Since $\vec{0} \in V$ is additive identity, then $\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}$ for all $\vec{v} \in V$.

Let $\vec{v} \in W$.

Since W is closed under scalar multiplication, and $0 \in F$ and $\vec{v} \in W$, then $0 \cdot \vec{v} \in W$, so $\vec{0} \in W$, by theorem 2.

Since $\vec{0} \in W$, and $\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}$ for all $\vec{v} \in V$, then $0 \in W$ is additive identity.

Let $\vec{v} \in W$.

Since $\vec{v} \in W$ and $W \subset V$, then $\vec{v} \in V$.

Since every vector in V has an additive inverse in V, then there exists $-\vec{v} \in V$ such that $\vec{v} + (-\vec{v}) = -\vec{v} + \vec{v} = \vec{0}$.

Since W is closed under scalar multiplication, and $-1 \in F$ and $\vec{v} \in W$, then $(-1)\vec{v} \in W$, so $-\vec{v} \in W$, by theorem 2.

Hence, there exists $-\vec{v} \in W$ such that $\vec{v} + (-\vec{v}) = -\vec{v} + \vec{v} = \vec{0}$, so for every $\vec{v} \in W$, there exists $-\vec{v} \in W$ such that $\vec{v} + (-\vec{v}) = -\vec{v} + \vec{v} = \vec{0}$.

Therefore, every vector in W has an additive inverse in W.

Since associativity of scalar multiplication with field multiplication holds, then $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$ for all $\vec{v} \in V$ and for all $\alpha, \beta \in F$.

Let $\vec{v} \in W$.

Since $\vec{v} \in W$ and $W \subset V$, then $\vec{v} \in V$, so $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$ for all $\alpha, \beta \in F$.

Therefore, $\alpha(\beta\vec{v}) = (\alpha\beta)\vec{v}$ for all $\vec{v} \in W$ and for all $\alpha, \beta \in F$, so associativity of scalar multiplication with field multiplication holds in W.

Since the left distributive law of scalar multiplication over vector addition holds, then $\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$ for all $\vec{v}, \vec{w} \in V$ and for all $\lambda \in F$.

Let $\vec{v}, \vec{w} \in W$.

Since $\vec{v}, \vec{w} \in W$ and $W \subset V$, then $\vec{v}, \vec{w} \in V$, so $\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$ for all $\lambda \in F$.

Therefore, $\lambda(\vec{v} + \vec{w}) = \lambda\vec{v} + \lambda\vec{w}$ for all $\vec{v}, \vec{w} \in W$ and for all $\lambda \in F$, so the left distributive law of scalar multiplication over vector addition holds in W.

Since the right distributive law of scalar multiplication over scalar addition holds, then $(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$ for all $\vec{v} \in V$ and for all $\alpha, \beta \in F$.

Let $\vec{v} \in W$.

Since $\vec{v} \in W$ and $W \subset V$, then $\vec{v} \in V$, so $(\alpha+\beta)\vec{v} = \alpha\vec{v}+\beta\vec{v}$ for all $\alpha, \beta \in F$.

Therefore, $(\alpha + \beta)\vec{v} = \alpha\vec{v} + \beta\vec{v}$ for all $\vec{v} \in W$ and for all $\alpha, \beta \in F$, so the right distributive law of scalar multiplication over scalar addition holds in W.

Since $1 \in F$ is a multiplicative identity for scalar multiplication, then $1 \cdot \vec{v} = \vec{v}$ for all $\vec{v} \in V$.

Let $\vec{v} \in W$.

Since $\vec{v} \in W$ and $W \subset V$, then $\vec{v} \in V$, so $1 \cdot \vec{v} = \vec{v}$.

Therefore, $1 \cdot \vec{v} = \vec{v}$ for all $\vec{v} \in W$, so $1 \in F$ is a multiplicative identity for scalar multiplication in W.

Since W is closed under vector addition, and vector addition over W is associative, and vector addition over W is commutative, and $0 \in W$ is additive identity, and every vector in W has an additive inverse in W, and W is closed under scalar multiplication, and associativity of scalar multiplication with field multiplication holds in W, and the left distributive law of scalar multiplication over vector addition holds in W, and the right distributive law of scalar multiplication over scalar addition holds in W, and $1 \in F$ is a multiplicative identity for scalar multiplication in W, then $(W, +, \cdot)$ is a vector space.

Since $W \subset V$ and $(W, +, \cdot)$ is a vector space, then W is a subspace of V, as desired. □

Proof. Conversely, suppose W is a subspace of V.

Then $(W, +, \cdot)$ is a vector space under vector addition and scalar multiplication defined on V, so vector addition $W \times W \to W$ is a binary operation on W, and scalar multiplication $F \times W \to W$ is a function.

Therefore, W is closed under vector addition and scalar multiplication. □

TODO: Rework the below sections.

1 Matrix Theory

Proposition 4. *Let $n \in \mathbb{Z}^+$.*

Let A be a $n \times n$ matrix and I be the identity matrix.

Then $A = AI$.

Solution. Hypothesis is: A is a $n \times n$ matrix.

Conclusion is: $A = AI$.

To prove $A = AI$, we must prove

$(\forall i \in \mathbb{N}_n)(\forall j \in \mathbb{N}_n)(a_{ij} = b_{ij})$, where $A = (a_{ij})_{n\times n}$ and $AI = (b_{ij})_{n\times n}$ and $(b_{ij}) = \sum_{k=1}^{n} a_{ik}\delta_{kj}$.

We can work through examples and see that each entry a_{ij} will be $a_{ij} \cdot 1$ when we're in the k^{th} row and column of I and zero everywhere else. So, the key idea is either $k = j$ or not, based on the definition of I. □

Proof. Let i and j be arbitrary elements of $\mathbb{N}_n$. Let $A = (a_{ij})_{n\times n}$. Let $AI = (b_{ij})_{n\times n}$ where $b_{ij} = \sum_{k=1}^{n} a_{ik}\delta_{kj}$ and $\delta_{ij} = 1$ whenever $i = j$ and $\delta_{ij} = 0$ whenever $i \neq j$.

To prove $a_{ij} = b_{ij}$, we must prove $a_{ij} = \sum_{k=1}^{n} a_{ik}\delta_{kj}$.

Let $k \in \mathbb{N}_n$. Either $k = j$ or $k \neq j$.

We consider these cases separately.

Suppose $k = j$. Then $a_{ik}\delta_{kj} = a_{ij}\delta_{jj} = a_{ij}(1) = a_{ij}$.

Suppose $k \neq j$. Then $a_{ik}\delta_{kj} = a_{ik}(0) = 0$.

Hence, the term $a_{ik}\delta_{kj}$ is either a_{ij} or zero.

Since $\sum_{k=1}^{n} a_{ik}\delta_{kj}$ is the sum of n of these terms, then $\sum_{k=1}^{n} a_{ik}\delta_{kj}$ is the sum of a_{ij} and $n-1$ zeroes. Thus, $\sum_{k=1}^{n} a_{ik}\delta_{kj} = a_{ij} + (n-1)(0) = a_{ij}$, as desired. □

Proposition 5. *Let $n \in \mathbb{Z}^+$. Let S be the set of all invertible $n \times n$ matrices. Let $\cdot$ represent matrix multiplication. Then $(S, \cdot)$ is a non-abelian group.*

Solution. To prove $(S, \cdot)$ is a group we must prove:

1. $\cdot$ is a binary operation on S.
2. $\cdot$ is associative.
3. there exists a multiplicative identity in S.
4. each element of S has a multiplicative inverse in S.

To prove 1 we must prove: $\cdot : S \times S \mapsto S$ is a function; that is, we must prove

1a. S is closed under $\cdot$, that is, $(\forall A, B \in S)(AB \in S)$.

1b. AB is unique.

To prove 1a, let $A, B \in S$ be arbitrary. To prove $AB \in S$, we must prove 1a.1 AB is an $n \times n$ matrix we can prove this by showing that A and B are $n \times n$ matrices.

1a.2 AB is invertible, that is, there exists matrix C such that $(AB)C = C(AB) = I$.

To find C, we work backwards. Suppose $(AB)C = I$. Solve for C. To do this, we have $A(BC) = I$. We must have A^{-1} exist, so that $(A^{-1}A)(BC) = A^{-1}I$, so $BC = A^{-1}$. We must have B^{-1} exist, so that $(B^{-1}B)C = B^{-1}A^{-1}$, so $IC = B^{-1}A^{-1}$, so $C = B^{-1}A^{-1}$.

Thus, we must show A^{-1} and B^{-1} exist, and let $C = B^{-1}A^{-1}$.

To prove 3, we must find an element $e \in S$ such that for every $a \in S$, $ea = ae = a$.

We work backwards. Suppose $EA = A$ for some $n \times n$ invertible matrix A. We know identity matrix satisfies this equation. Thus, let $E = I$. Now, we must prove I is in S; that is, prove I is $n \times n$ matrix and I is invertible.

To prove 4, we must prove $(\forall a \in S)(\exists a^{-1} \in S)(aa^{-1} = a^{-1}a = e)$.

□

Proof. Let $n \in \mathbb{Z}^+$. Let $S = \{X : X \text{ is an } n \times n \text{ invertible matrix } \}$. Let $\cdot$ represent matrix multiplication.

We prove $\cdot$ is a binary operation on S.

Let A and B be arbitrary $n \times n$ invertible matrices. Then A and B are $n \times n$ matrices. Therefore, AB is an $n \times n$ matrix.

Since A is invertible, then A^{-1} exists and A^{-1} is an $n \times n$ matrix. Since B is invertible, then B^{-1} exists and B^{-1} is an $n \times n$ matrix. Hence, the product $B^{-1}A^{-1}$ exists and $B^{-1}A^{-1}$ is an $n \times n$ matrix.

Let $C = B^{-1}A^{-1}$. Then C is an $n \times n$ matrix.

Observe that

$$\begin{aligned}(AB)C &= (AB)(B^{-1}A^{-1}) \\ &= A(BB^{-1})A^{-1} \\ &= AIA^1 \\ &= AA^{-1} \\ &= I\end{aligned}$$

and

$$\begin{aligned}C(AB) &= (B^{-1}A^{-1})(AB) \\ &= B^{-1}(A^{-1}A)B \\ &= B^{-1}IB \\ &= B^{-1}B \\ &= I\end{aligned}$$

Therefore, AB is invertible.

Since AB is an $n \times n$ matrix and AB is invertible, then $AB \in S$.

Therefore, S is closed under $\cdot$.

Since the product of two $n \times n$ matrices is a unique matrix, then, in particular, AB is unique.

Thus, $\cdot$ is a binary operation on S.

Since matrix multiplication is associative in general, then in particular, matrix multiplication is associative in S.

We prove there exists a multiplicative identity in S. Let I be the $n \times n$ identity matrix. Suppose A is an arbitrary $n \times n$ invertible matrix. Then $AI = IA = A$. Since $I = I \cdot I$, then I is invertible. Since I is invertible and I is an $n \times n$ matrix, then $I \in S$. Therefore, S has a multiplicative identity, namely, I, as desired.

We prove each element of S has a multiplicative inverse. Let A be an arbitrary $n \times n$ invertible matrix. We must prove there exists some $B \in S$ such that $AB = BA = I$.

Since A is an invertible $n \times n$ matrix, then A^{-1} exists and A^{-1} is an $n \times n$ matrix. Let $B = A^{-1}$. Then $AB = AA^{-1} = I = A^{-1}A = BA$, as desired. Thus, A^{-1} is a multiplicative inverse of A.

To prove $A^{-1} \in S$, we must find some $C \in S$ such that $A^{-1}C = CA^{-1} = I$. Let $C = A$. Since $A \in S$, then $C \in S$. Observe that $A^{-1}C = A^{-1}A = I = AA^{-1} = CA^{-1}$. Hence, $A^{-1} \in S$. Since A^{-1} is a multiplicative inverse of A and $A^{-1} \in S$, then A has a multiplicative inverse in S. Since A is arbitrary, then every $A \in S$ has a multiplicative inverse in S.

Therefore, $(S, \cdot)$ is a group.

Since matrix multiplication is not commutative (in general), then matrix multiplication is not commutative, in particular, in S, in general.

Hence, $(S, \cdot)$ is a non-abelian multiplicative group.

We call S the **general linear group of degree** n and denote it by GL_n. □

2 Vector Space Theorems

Proposition 6. *The empty set is linearly independent.*

Solution. Let $\emptyset$ be the empty set. To prove $\emptyset$ is linearly independent, we use proof by contradiction. Thus, we suppose $\emptyset$ is linearly dependent.

Let V be a vector space over a field K.

If $\emptyset$ is linearly dependent, then by definition of linear dependence, $(\exists_{k=1}^{n} \alpha_k \in K)[(\sum_{k=1}^{n} \alpha_k \vec{v}_k = \vec{0}) \wedge (\exists_{k=1}^{n} k)(\alpha_k \neq 0)]$.

We analyze these quantified expressions.

Observe that $\exists_{k=1}^{n} \alpha_k \in K \Leftrightarrow (\exists_{k=1}^{n} k)(\alpha_k \in K)$.

This implies the existence of a function that assigns to each index k a value α_k. Observe that each k is contained in $\mathbb{N}_n$ where $\mathbb{N}_n = \{1, 2, ..., n\}$ and each α_k is contained in K.

Define $f : \mathbb{N}_n \mapsto K$ by $f(k) = \alpha_k$. Then function f assigns to each $k \in \mathbb{N}_n$ a unique $\alpha_k \in K$.

Hence, to each index $k \in \mathbb{N}_n$ there exists a unique scalar $\alpha_k \in K$.

The expression $(\sum_{k=1}^{n} \alpha_k \vec{v}_k = \vec{0}) \wedge (\exists_{k=1}^{n} k)(\alpha_k \neq 0)$ means that the linear combination of vectors in $\emptyset$ equals the zero vector and at least one $k \in \mathbb{N}_n$ exists such that $\alpha_k \neq 0$.

Thus, if $\emptyset$ is linearly dependent, then there exists some index $k \in \mathbb{N}_n$ such that to this k, a nonzero scalar $\alpha_k \in K$ can be assigned for which the linear combination of vectors in $\emptyset$ equals the zero vector.

But, $\emptyset$ is empty, so there are no vectors in $\emptyset$. Hence, there is no index k to choose to assign a nonzero scalar α_k such that the linear combination of vectors in $\emptyset$ equals the zero vector. Thus, no such index k exists. Hence, $\emptyset$ cannot be linearly dependent. Thus, $\emptyset$ is linearly independent.

□

Proof. Let $\emptyset$ be the empty set in a vector space over a field K.

Suppose $\emptyset$ is linearly dependent. Let $\mathbb{N}_n = \{1, 2, ..., n\}$. Then there exists some index $k \in \mathbb{N}_n$ such that to this k, a nonzero scalar $\alpha_k \in K$ can be assigned for which the linear combination of vectors in $\emptyset$ equals the zero vector.

Since $\emptyset$ is empty, then there are no vectors in $\emptyset$.

Hence, it is impossible to choose an index k such that to k, a nonzero scalar $\alpha_k \in K$ can be assigned for which the linear combination of vectors in $\emptyset$ equals the zero vector. Thus, no such index k exists. Since there exists such an index k and there does not exist such an index k, we have a contradiction. Hence, $\emptyset$ cannot be linearly dependent. Therefore, $\emptyset$ must be linearly independent. $\square$

Proposition 7. *Let T be a set of linearly independent vectors. Let S be a subset of T. Then S is linearly independent.*

Solution. Our hypothesis is T is a linearly independent set of vectors and $S \subseteq T$. To prove our conclusion S is linearly independent, we must prove $(\forall_{k=1}^{n}\alpha_k \in K)[(\sum_{k=1}^{n} \alpha_k\vec{v}_k = \vec{0}) \rightarrow (\forall_{k=1}^{n}k)(\alpha_k = 0)]$.

Since T is a linearly independent set of vectors, then T is a finite set of vectors. Let n be the cardinality of T. Then $n \geq 0$. Let $T = \{\vec{v}_1, \vec{v}_2, ..., \vec{v}_n\}$.

Since S is a subset of T, then either $S = \emptyset$ or $S = T$ or S is a proper subset of T.

We consider these cases separately.

Case 1: Suppose $S = \emptyset$.

Since $\emptyset$ is linearly independent and $S = \emptyset$, then S is linearly independent.

Case 2: Suppose $S = T$.

By hypothesis, T is linearly independent. Since $S = T$, then S is linearly independent.

Case 3: Suppose S is a proper subset of T.

Then S contains at least one vector of T but no more than n vectors of T. Let k be the cardinality of S. Then $1 \leq k < n$.

Since S is arbitrary, let $S = \{\vec{v}_1, \vec{v}_2, ..., \vec{v}_k\}$ where each $\vec{v}_i \in T$.

To prove S is linearly independent, we must prove $(\forall_{i=1}^{k}\alpha_i \in K)[(\sum_{i=1}^{k} \alpha_i\vec{v}_i = \vec{0}) \rightarrow (\forall_{i=1}^{k}i)(\alpha_i = 0)]$.

Let $\alpha_1, \alpha_2, ..., \alpha_k$ be k arbitrary elements of K such that $\sum_{i=1}^{k} \alpha_i\vec{v}_i = \vec{0}$.

We must prove $(\forall_{i=1}^{k}i)(\alpha_i = 0)$; that is, we must show that $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$.

Since T is linearly independent, then $(\forall_{k=1}^{n}\alpha_k \in K)[(\sum_{k=1}^{n} \alpha_k\vec{v}_k = \vec{0}) \rightarrow (\forall_{k=1}^{n}k)(\alpha_k = 0)]$.

Hence, $(\exists_{k=1}^{n}\alpha_k \in K)[(\sum_{k=1}^{n} \alpha_k\vec{v}_k = \vec{0}) \rightarrow (\forall_{k=1}^{n}k)(\alpha_k = 0)]$.

Therefore, $\sum_{k=1}^{n} \alpha_k\vec{v}_k = \vec{0} \Rightarrow (\forall_{k=1}^{n}k)(\alpha_k = 0)]$ for arbitrary $\alpha_1, \alpha_2, ..., \alpha_n$ elements of K.

Thus, let $\alpha_1, \alpha_2, ..., \alpha_n$ be n arbitrary elements of K such that $\sum_{k=1}^{n} \alpha_k\vec{v}_k = \vec{0}$.

Then $(\forall_{k=1}^{n}k)(\alpha_k = 0)$, so $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$.

Observe that $\vec{0} = \sum_{k=1}^{n} \alpha_k\vec{v}_k = \sum_{i=1}^{n} \alpha_i\vec{v}_i = \sum_{i=1}^{k} \alpha_i\vec{v}_i + \sum_{i=k+1}^{n} \alpha_i\vec{v}_i$.

Suppose $\sum_{i=1}^{k} \alpha_i\vec{v}_i = \vec{0}$. We must prove $(\forall_{i=1}^{k}i)(\alpha_i = 0)$; that is, we must show that $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$.

Since $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$, then $\alpha_1 = \alpha_2 = ... = \alpha_k = \alpha_{k+1} = ... = \alpha_n = 0$. Therefore, $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$, as desired. $\square$

Proof. Let T be a set of linearly independent vectors. Let S be a subset of T.

Since T is a linearly independent set of vectors, then T is a finite set of vectors.

Let $n \in \mathbb{Z}$ be the cardinality of T. Then $n \geq 0$.

Let $T = \{\vec{v}_1, \vec{v}_2, ..., \vec{v}_n\}$.

Since S is a subset of T, then either $S = \emptyset$ or $S = T$ or S is a proper subset of T.

We consider these cases separately.

Case 1: Suppose $S = \emptyset$.

Since $\emptyset$ is linearly independent and $S = \emptyset$, then S is linearly independent.

Case 2: Suppose $S = T$.

By hypothesis, T is linearly independent. Since $S = T$, then S is linearly independent.

Case 3: Suppose S is a proper subset of T.

Then S contains at least one vector of T but no more than n vectors of T. Let $k \in \mathbb{Z}$ be the cardinality of S. Then $1 \leq k < n$.

Since S is arbitrary, let $S = \{\vec{v}_1, \vec{v}_2, ..., \vec{v}_k\}$ where each $\vec{v}_i \in T$.

To prove S is linearly independent, we must prove $(\forall_{i=1}^{k} \alpha_i \in K)[(\sum_{i=1}^{k} \alpha_i \vec{v}_i = \vec{0}) \rightarrow (\forall_{i=1}^{k} i)(\alpha_i = 0)]$.

Since T is linearly independent, then $(\forall_{k=1}^{n} \alpha_k \in K)[(\sum_{k=1}^{n} \alpha_k \vec{v}_k = \vec{0}) \rightarrow (\forall_{k=1}^{n} k)(\alpha_k = 0)]$.

Let $\alpha_1, \alpha_2, ..., \alpha_n$ be n arbitrary elements of K such that $\sum_{k=1}^{n} \alpha_k \vec{v}_k = \vec{0}$.

Then $(\forall_{k=1}^{n} k)(\alpha_k = 0)$, so $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$.

Observe that $\vec{0} = \sum_{k=1}^{n} \alpha_k \vec{v}_k = \sum_{i=1}^{n} \alpha_i \vec{v}_i = \sum_{i=1}^{k} \alpha_i \vec{v}_i + \sum_{i=k+1}^{n} \alpha_i \vec{v}_i$.

Since $\alpha_1, \alpha_2, ..., \alpha_n$ are n arbitrary elements of K and $k < n$, then $\alpha_1, \alpha_2, ..., \alpha_k$ are k arbitrary elements of K.

Suppose $\sum_{i=1}^{k} \alpha_i \vec{v}_i = \vec{0}$. To prove $(\forall_{i=1}^{k} i)(\alpha_i = 0)$, we must show that $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$.

Since each of the n α_i is zero and $k < n$, then each of the k α_i must be zero. Therefore, $\alpha_1 = \alpha_2 = ... = \alpha_k = 0$, as desired.

Since S and T are arbitrary, then a subset of a linearly independent set of vectors is linearly independent. □

Proposition 8. *Let S be a set of linearly dependent vectors. Let T be a superset of S. Then T is linearly dependent.*

Solution. Hypothesis is: $T \supset S$.

Conclusion is: if S is linearly dependent, then T is linearly dependent.

Directly proving that T is linearly dependent using the definition of linear dependence does not lead anywhere, so we must try a different approach. We will use indirect proof using contrapositive.

Thus, we assume T is linearly independent. We must prove S is linearly independent.

How can we show S is linearly independent? We know $T \supset S$, so $S \subset T$.

We also proved that a subset of a linearly independent set must be linearly independent. Hence, since T is linearly independent and $S \subset T$, then S is linearly independent, as desired.

This proposition states that a superset of a linearly dependent set of vectors is linearly dependent. □

Proof. To prove S is linearly dependent implies T is linearly dependent, we prove T is linearly independent implies S is linearly independent.

Suppose T is linearly independent. We must prove S is linearly independent.

Since T is a superset of S, then S is a subset of T. A subset of a linearly independent set of vectors is linearly independent. Since $S \subset T$ and T is linearly independent, then we conclude S is linearly independent, as desired. □

Proposition 9. *Let V and W be vector spaces over a field K.*
Let T be a linear transformation from V to W.
Let $\vec{v}, \vec{w} \in V$ be arbitrary.
Let $\alpha, \beta \in K$ be arbitrary.
Then the following are true:
1. $T(\alpha\vec{v} + \beta\vec{w}) = \alpha T(\vec{v}) + \beta T(\vec{w})$.
2. $T(\vec{0}) = \vec{0}$.
3. $T(\vec{u} - \vec{v}) = T\vec{u} - T\vec{v}$.

Proof. Let V and W be vector spaces over a field K.
Let $T : V \mapsto W$ be a linear transformation.
Let $\vec{v}, \vec{w} \in V$ be arbitrary.
Let $\alpha, \beta \in K$ be arbitrary.

Observe that

$$\begin{aligned} T(\alpha\vec{v} + \beta\vec{w}) &= T(\alpha\vec{v}) + T(\beta\vec{w}) \\ &= \alpha T(\vec{v}) + \beta T(\vec{w}) \end{aligned}$$

Therefore, $T(\alpha\vec{v} + \beta\vec{w}) = \alpha T(\vec{v}) + \beta T(\vec{w})$.

Observe that

$$\begin{aligned} \vec{0} &= T(\vec{0}) - T(\vec{0}) \\ &= T(\vec{0} + \vec{0}) - T(\vec{0}) \\ &= T(\vec{0}) + T(\vec{0}) - T(\vec{0}) \\ &= T(\vec{0}) + \vec{0} \\ &= T(\vec{0}) \end{aligned}$$

Therefore, $T(\vec{0}) = \vec{0}$.

Observe that

$$\begin{aligned} T(\vec{u}-\vec{v}) &= T(\vec{u}+\vec{-v}) \\ &= T(\vec{u})+T(-\vec{v}) \\ &= T(\vec{u})+T((-1)\vec{v}) \\ &= T(\vec{u})+(-1)T(\vec{v}) \\ &= T\vec{u}-T\vec{v} \end{aligned}$$

Therefore, $T(\vec{u}-\vec{v}) = T\vec{u}-T\vec{v}$.

□