Vector Spaces.

Overview:

In this part of the course we study about "vector spaces" (or linear spaces) over a given field F. Of course, you have learned about "vectors", to some extent, in your A/L classes. The vectors you studied there most often had a magnitude and a direction. Indeed, there you defined a vector as an "object" which has both a magnitude and a direction. In this course, however, you will see that a vector is defined as an element of a vector space. This implicitly says that some vectors we will be studying of do not have a magnitude or a direction that we know of.

A vector space consists of a nonempty set, which is usually denoted by V and the objects in which are called 'vectors', a field F, elements in which are called scalars and two binary operations satisfying certain properties called as axioms.

In the study of vectors, at the beginning, we want to fix a field (we will shortly define a field rigorously) such as the field of real numbers, field of complex numbers, etc. We then consider vector spaces over that field. It is one of the prime ingredients in defining a vector space.

Roughly speaking, a field is a set F together with some operations on the objects in that set satisfying certain conditions. These operations behave like ordinary addition, subtraction, multiplication, and division of real numbers.

The two binary operations are vector addition, denoted by $+$, and scalar multiplication, denoted by $\cdot$. $+$ is a function from $V \times V$ into V and $\cdot$ is a function from $F \times V$ into V, where V is the set of vectors and F is the set of scalars (which is the field) under consideration.

Some common choices for F are $\mathbb{R}$ - the field of real numbers, $\mathbb{C}$ - the field of complex numbers, $\mathbb{Q}$ - the field of rational numbers. F could be a finite field like $\mathbb{Z}_p$ - the integers modulo p; where p is a prime, as well.

These two operations allow us to add two vectors and to multiply a vector by a scalar. You have learned in your A/L classes that vectors can be added and can be scalar multiplied, where scalars are the real (or complex) numbers.

For each $u, v \in V$, the image of $(u,v) \in V \times V$ under $+$, i.e. $+(u,v)$, is usually denoted by $u+v$. It is called the 'sum' of u and v. For each $\alpha \in F$ and $v \in V$, the image of $(\alpha, v) \in F \times V$ under $\cdot$, i.e. $\cdot(\alpha, v)$, is usually denoted by $\alpha \cdot v$ or simply αv. It is called the 'product' of α and v.

The most important thing about vector addition is that V is closed under addition $+$. That is, when you add two vectors you again get a vector in V. That is, for each $u, v \in V$, $u+v \in V$. The most important thing about scalar multiplication is that V is closed under scalar multiplication $\cdot$. That is, when you left multiply a vector by a scalar, you again get a vector in V. That is, for each $\alpha \in F$ and $v \in V$, $\alpha v \in V$.

If a and b are numbers, then you can left multiply b by a to get ab or you can right multiply b by a to get ba. Both ab an ba are meaningful: However, when comes to scalar multiplication, a vector can be multiplied by a scalar from the left only. Thus, $v\alpha$ does NOT have a meaning, where $v \in V$ and $\alpha \in F$.

These two operations cannot be arbitrarily defined. As it was mentioned earlier, these two operations should satisfy certain condition-s. When the two operations satisfy these conditions, the entire algebraic system (or the algebraic structure) $(V, F, + : V \times V \to V, \cdot : F \times V \to V)$ is called as a vector space over F. This is the minimal set up to study vectors.

An algebraic system richer in its structure than a vector space is "normed vector space". A normed vector space is a vector space V together with a real valued function on V called "norm" satisfying certain conditions. This function allows one to assign a magnitude to each vector in V. Thus, we identify vectors with a magnitude as elements in a normed vector space.

An even richer algebraic system is "inner product space". This is also a a vector space together with a scalar valued function on $V \times V$ called "inner product on V" satisfying certain conditions. We identify vectors with a magnitude and a direction as elements in an inner product space. We will discuss about inner product spaces at the latter part of this section.

We often want to study about "structure preserving" mappings between two vector spaces. The structure preserving mappings between vector spaces over a fixed field are called "Linear transformations", or given some extra assumptions what is well known "matrices". By doing this, we will bind our study of vector spaces closely with matrices.

Let's delve into these topics one by one.

We start with the definition of a field.

Definition 1: A field F is a nonempty set with two binary operations on F, called addition - denoted by $+$, and multiplication - denoted by $\cdot$, satisfying the following conditions (or axioms)

(i). For each $a, b \in F$, $a+b = b+a$ (that is, addition is commutative)

(ii). For each $a, b, c \in F$, $a+(b+c) = (a+b)+c$ (that is, addition is associative).

(iii). There exists $0 \in F$ (called "zero") such that for each $a \in F$, $a+0 = a$.

(iv). For each $a \in F$, there exist $-a \in F$ such that $a+(-a) = 0$.

(v). For each $a, b \in F$, $a b = b \cdot a$ (that is, multiplication is commutative).

(vi). For each $a, b, c \in F$, $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ (that is multiplication is associative)

(vii). There exists a nonzero element $1 \in F$ (called "one") such that for each $a \in F$, $a \cdot 1 = a$.

(viii). For each nonzero $a \in F$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

(ix). For each $a, b, c \in F$, $a\cdot(b+c) = a\cdot b + a\cdot c$ (that is, multiplication distributes over addition).

Note: Recall that a binary operation on a set A is a function f from $A \times A$ into A. Thus, you should understand that for each $a, b \in F$, $a+b \in F$ and $a\cdot b \in F$. In other words F is closed under addition and F is closed under multiplication.

You can easily verify the following for a field F.

1). $0 \in F$ is unique. 0 (zero) is sometimes called the additive identity.

2). For each $a \in F$, $-a$ is unique. $-a$ is sometimes called the additive inverse of a.

3). $1 \in F$ is unique. 1 (one) is sometimes called the multiplicative identity.

4). For each $a (\neq 0) \in F$, a^{-1} is unique. a^{-1} is sometimes called the multiplicative inverse of a.

Given a nonempty set F and two binary operations, addition and multiplication, on F, to show that F is a field, you need to verify that the two binary operations satisfy all the 9 conditions (or axioms) listed above. If at least one condition is not satisfied, then F is not a field under the given two operations.

Examples:

1). The set of all real numbers $\mathbb{R}$, under usual addition and multiplication is a field.

2). The set of all rational numbers $\mathbb{Q}$, is a field under usual addition and multiplication.

3). The set of all complex numbers $\mathbb{C}$, is a field under usual addition of complex numbers and the usual multiplication of complex numbers.

4). $\{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field under usual addition of real numbers and the usual multiplication of real numbers.

It is not necessary that the addition and the multiplication in a field to be the usual addition and the usual multiplication that we know of as in the four examples above. Also, it is not necessary that the additive identity and the multiplicative identity of a field to be the real 0 and 1 we know of even if we use the same symbols to denote the additive identity and the multiplicative identity of an arbitrary field F respectively.

The following example illustrates this situation.

5. For each $a, b \in \mathbb{Q}$, define addition, $+$, and multiplication, $\cdot$, in the following way.

$a + b = a + b - 1$ and $a \cdot b = a + b - ab$. Prove that $\mathbb{Q}$ is a field under the addition and the multiplication defined above.

Solution: First, note that the addition on the left hand side of the equation $a+b = a+b-1$ is not the same as the addition on the right hand side of the equation. The addition and the subtraction on the right hand side of the equation are the usual ones. Also, the multiplication on the left hand side of the equation $a \cdot b = a+b-ab$ is not the same as the multiplication on the right hand side of the equation. The addition, subtraction and the multiplication appears on the right hand of the equation are the usual ones.

Now, let's prove that $\mathbb{Q}$ under the addition and the multiplication defined above is a field. To this end, we must verify all the 9 axioms listed in the definition of a field.

Clearly $\mathbb{Q} \neq \emptyset$.

Let $a, b \in \mathbb{Q}$. Note that $a+b = a+b-1 = b+a-1 = b+a$. Thus, $+$ is commutative.

Now let $a, b, c \in \mathbb{Q}$. Note that $a+(b+c) = a+(b+c-1) = a+(b+c-1)-1$
$= a+b+c-2$ and $(a+b)+c = (a+b-1)+c = (a+b-1)+c-1 = a+b+c-2$.

Thus, $a+(b+c) = (a+b)+c$. That is $+$ is associative.

Observe that $1 \in \mathbb{Q}$ and for each $a \in \mathbb{Q}$, $a+1 = a+1-1 = a$. So, 1 is the additive identity (or zero)!

Now let $a \in \mathbb{Q}$. Then $-a+2 \in \mathbb{Q}$ (here $+$ is the usual addition). Note that $a \oplus (-a+2) = a + (-a+2) - 1 = a - a + 2 - 1 = 1$. Thus, $-a+2$ is the additive inverse of a.

Let $a, b \in \mathbb{Q}$. Observe that $a \cdot b = a + b - ab = b + a - b \cdot a = b \cdot a$. Thus, $\cdot$ is commutative.

Let $a, b, c \in \mathbb{Q}$. Note that $(a \cdot b) \cdot c = (a+b-ab) \cdot c = (a+b-ab) + c - (a+b-ab)c = a + b + c - ab - ac - bc + abc$ and $a \cdot (b \cdot c) = a \cdot (b+c-bc) = a + (b+c-bc) - a(b+c-bc) = a+b+c-ab-ac-bc+abc$. Hence, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. So, $\cdot$ is associative.

Observe that $0 \in \mathbb{Q}$ and for each $a \in \mathbb{Q}$, $a \cdot 0 = a + 0 - a \cdot 0 = a$. Thus, 0 is the multiplicative identity or "one"!

Now let $a \in \mathbb{Q}$. Assume $a \neq 1$ (the zero). Then $\frac{-a}{1-a} \in \mathbb{Q}$. Notice that $a \cdot \left(\frac{-a}{1-a}\right) = a + \frac{-a}{1-a} - a\left(\frac{-a}{1-a}\right) = \frac{a - a^2 - a + a^2}{1-a} = 0$ (the multiplicative identity). Thus, $\frac{-a}{1-a}$ is the multiplicative inverse of a.

Finally, let $a, b, c \in \mathbb{Q}$. Note that $a \cdot (b \oplus c) = a \cdot (b + c - 1) = a + b + c - 1 - a(b+c-1) = a + b + c - 1 - ab - ac + a = (a + b - ab) + (a + c - ac) - 1 = (a \cdot b) + (a \cdot c) - 1 = (a \cdot b) \oplus (a \cdot c)$. Thus, $\cdot$ is distributive over $\oplus$.

Therefore, $\mathbb{Q}$ is a field under the addition and the multiplication defined above.

Example 6: For each $a, b \in \mathbb{Z}$, define addition, $+$, and multiplication, $\cdot$, in the following way.

$a + b = a + b - 1$ and $a \cdot b = a + b - ab$. Prove that $\mathbb{Z}$ with addition and multiplication defined above is not a field. (Check each condition one by one).

Definition 2: Let F be a field and let $E \neq \emptyset$ be a subset of F. E is said to be a subfield of F if E itself is a field under the addition and multiplication in F.

Examples:

1). Under usual addition and multiplication both $\mathbb{R}$ and $\mathbb{Q}$ are subfields of $\mathbb{C}$.

2). The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with usual addition and multiplication is a subfield of both $\mathbb{R}$ and $\mathbb{C}$.

3). The set of positive integers, $\mathbb{Z}^+$ and the set of integers $\mathbb{Z}$ are not subfields of $\mathbb{R}$ under usual addition and multiplication.

With that we end our discussion about fields. Let's move on to our main topic - Vector spaces.

Vector Spaces.

Definition 3 : A vector space over the field F is a nonempty set V together with two binary operations $+ : V \times V \rightarrow V$ and $\cdot : F \times V \rightarrow V$ satisfying the following axioms.

(i). For each $u, v \in V$, $u + v = v + u$.

(ii). For each $u, v, w \in V$, $(u+v)+w = u+(v+w)$.

(iii). There exist $0 \in V$ such that for each $v \in V$, $v + 0 = v$.

(iv). For each $v \in V$ there exists $-v \in V$ such that $v + (-v) = 0$

(v). For each $v \in V$, $1 \cdot v = v$.

(vi). For each $\alpha, \beta \in F$ and $v \in V$, $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$

(vii). For each $\alpha, \beta \in F$ and $v \in V$, $(\alpha+\beta) \cdot v = \alpha \cdot v + \beta \cdot v$

(viii). For each $\alpha \in F$ and $u, v \in V$, $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$.

Note :- When there is no chance of confusion, we may simply refer to the vector space as V, or when it is desirable to specify the field, we shall say V is a vector space over the field F.

- $+$ is called as vector addition and $\cdot$ is called as scalar multiplication.
- V is closed under addition and scalar multiplication.
- Elements in F are called scalars and elements in V are called vectors.

- In this course, for the most part, we will take scalars to be real or complex numbers. That is $F = \mathbb{R}$ or $F = \mathbb{C}$. If $F = \mathbb{R}$, then V is a real vector space and if $F = \mathbb{C}$, then V is a complex vector space.

- It is important to note that there is a zero element in F as well. We have used the same symbol '0' to denote the zero vector in V. To avoid this, some authors use $\underset{\sim}{0}$ to denote the zero vector in V. However, in this course we will use 0 to denote zero vector and the two zeros can be identified or distinguished from the context.

- The vector $-v$ is called the additive inverse of $v \in V$.

Before giving some examples for vector spaces, it is worth having the following results first.

Proposition 1: $0 \in V$ is unique.

Proof: Exercise.

Proposition 2: For each $v \in V$, $-v$ is unique.

Proof: Exercise.

Examples:

1). Let $n \geq 2$ be a positive integer. Let $\mathbb{R}^2 = \{(x,y) : x, y \in \mathbb{R}\}$ be the set of all 2-tuples of scalars in $\mathbb{R}$. For each $u = (x_1, y_1)$ and $v = (x_2, y_2)$ in $\mathbb{R}^2$ and $\alpha \in \mathbb{R}$, let $u + v = (x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ and $\alpha \cdot u = \alpha \cdot (x_1, y_1) = (\alpha x_1, \alpha y_1)$. With this vector addition and scalar multiplication, $\mathbb{R}^2$ is a vector space over $\mathbb{R}$.

Let's verify this. To this end, we need to show that the two binary operations satisfy all the 8 axioms listed in the definition of a vector space. Clearly $\mathbb{R}^2$ is closed under $+$ and $\cdot$.
Also, $\mathbb{R}^2 \neq \emptyset$ as $(0,0) \in \mathbb{R}^2$.
Let $u = (x_1, y_1)$, $v = (x_2, y_2) \in \mathbb{R}^2$. Then, $u + v = (x_1, y_1) + (x_2, y_2) =$
$(x_1 + x_2, y_1 + y_2) = (x_2 + x_1, y_2 + y_1) = (x_2, y_2) + (x_1, y_1) = v + u$.
Let $u = (x_1, y_1)$, $v = (x_2, y_2)$, $w = (x_3, y_3) \in \mathbb{R}^2$. Note that:
$(u+v) + w = [(x_1, y_1) + (x_2, y_2)] + (x_3, y_3) = (x_1 + x_2, y_1 + y_2) + (x_3, y_3)$
$= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) = (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) =$
$(x_1, y_1) + [(x_2, y_2) + (x_3, y_3)] = u + (v + w)$.

Clearly $(0,0) \in \mathbb{R}^2$ as $0 \in \mathbb{R}$. Note that for each $u = (x_1, y_1) \in \mathbb{R}^2$,
$u + (0,0) = (x_1, y_1) + (0,0) = (x_1 + 0, y_1 + 0) = (x_1, y_1) = u$. Thus,
$(0,0)$ is the zero vector in $\mathbb{R}^2$.
Let $v = (x_1, y_1) \in \mathbb{R}^2$. Note that $(-x_1, -y_1) \in \mathbb{R}^2$ and $(x_1, y_1) + (-x_1, -y_1) =$
$(x_1 - x_1, y_1 - y_1) = (0,0)$. Thus, $(-x_1, -y_1)$ is the additive inverse of v.

Let $u = (x_1, y_1) \in \mathbb{R}^2$. It is clear that $1 \cdot u = 1 \cdot (x_1, y_1) = (1 \cdot x_1, 1 \cdot y_1) = (x_1, y_1) = u$.

Let $u = (x_1, y_1) \in \mathbb{R}^2$ and $\alpha, \beta \in \mathbb{R}$. Note that $(\alpha\beta) \cdot u = (\alpha\beta) \cdot (x_1, y_1)$
$= \big((\alpha\beta)x_1, (\alpha\beta)y_1\big) = \big(\alpha(\beta x_1), \alpha(\beta y_1)\big) = \alpha \cdot (\beta x_1, \beta y_1) = \alpha \cdot (\beta u)$.

Also, $(\alpha+\beta) \cdot u = (\alpha+\beta) \cdot (x_1, y_1) = \big((\alpha+\beta)x_1, (\alpha+\beta)y_1\big) =$
$(\alpha x_1 + \beta x_1, \alpha y_1 + \beta y_1) = (\alpha x_1, \alpha y_1) + (\beta x_1, \beta y_1) = \alpha \cdot (x_1, y_1) + \beta (x_1, y_1)$
$= \alpha \cdot u + \beta \cdot u$.

Finally, let $\alpha \in \mathbb{R}$ and $u = (x_1, y_1), v = (x_2, y_2) \in \mathbb{R}^2$. Then,
$\alpha \cdot (u+v) = \alpha \cdot \big[(x_1, y_1) + (x_2, y_2)\big] = \alpha \cdot (x_1 + x_2, y_1 + y_2) =$
$\big(\alpha(x_1 + x_2), \alpha(y_1 + y_2)\big) = (\alpha x_1 + \alpha x_2, \alpha y_1 + \alpha y_2) = (\alpha x_1, \alpha y_1) + (\alpha x_2, \alpha y_2)$
$= \alpha \cdot (x_1, y_1) + \alpha \cdot (x_2, y_2) = \alpha \cdot u + \alpha \cdot v$.

We have shown that $+$ and $\cdot$ satisfy all the 8-axioms.
Thus, $\mathbb{R}^2$ is a vector space over $\mathbb{R}$.

Bellow are more examples for vector space.

2). $V = \mathbb{R}^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in \mathbb{R} \text{ for } i = 1, 2, \dots, n\}$, where n is a positive integer greater than or equal 2, the set of all n-tuples of scalars in $\mathbb{R}$, is a vector space over $\mathbb{R}$ under the addition $+$ and scalar multiplication $\cdot$ defined analogotously as in example 1. This vector space is referred to as the Euclidean space.

That is, for each $u = (x_1, x_2, \ldots, x_n)$, $v = (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n$ and for each $\alpha \in \mathbb{R}$,

$$u + v = (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

and $\alpha \cdot u = \alpha \cdot (x_1, x_2, \ldots, x_n) = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$.

More generally, for any field F, the set $V = F^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in F \text{ for } i = 1, 2, \ldots, n\}$ of all n-tuples of scalars in F is a vector space over F, where for each $u = (x_1, x_2, \ldots, x_n)$, $v = (y_1, y_2, \ldots, y_n) \in F^n$ and $\alpha \in F$,

$u + v = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ and $\alpha \cdot u = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n)$.

3). The set $V = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$ of all 2×2 matrices over $\mathbb{R}$ is a vector space over $\mathbb{R}$ under usual addition of matrices and scalar multiplication of matrices.

That is, for each $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in V$, where $a_i, b_i, c_i, d_i \in \mathbb{R}$ for $i = 1, 2$, and $\alpha \in \mathbb{R}$,

$$A + B = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \text{ and } \alpha \cdot A = \begin{bmatrix} \alpha a_1 & \alpha b_1 \\ \alpha c_1 & \alpha d_1 \end{bmatrix}.$$

Scanned with CamScanner

In general For any field F and $m, n \in \mathbb{Z}^+$ such that $m, n \geq 2$, the set of all $m \times n$ matrices over the field F is a vector space over F under usual addition and scalar multiplication of scalars. (For the clarity, for $A, B \in F^{m \times n}$ - the set of all $m \times n$ matrices over F - $(A+B)_{ij} = A_{ij} + B_{ij}$ and for $\alpha \in F$, $(\alpha A)_{ij} = \alpha . A_{ij}$).

4). Let $X \neq \emptyset$ and let $V = \{f : X \to \mathbb{R}\}$ - the set of all functions from X into $\mathbb{R}$. The sum of two vectors $f, g \in V$ is defined by $(f+g)(x) = f(x) + g(x)$, where $x \in X$ and the product of the scalar $\alpha \in \mathbb{R}$ and $f \in V$ is defined by $(\alpha f)(x) = \alpha f(x)$, where $x \in X$. Then V is a vector space over $\mathbb{R}$.

Indeed V can be the set of all functions f from X into the field F. In this case, V is a vector space over F. The addition in $f(x) + g(x)$ is the addition in F and the product in $\alpha . f(x)$ is the multiplication in F.

5). The set V of all polynomial functions over $\mathbb{R}$,

$V = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \mid n \in \mathbb{Z}^+ \cup \{0\}, a_i \in \mathbb{R}$ for $i = 0, 1, 2, \dots, n-1, n \}$ is a vector space over $\mathbb{R}$ under usual addition and scalar multiplication of functions.

6). Let F be a field and E be a subfield of F. Then, F is a vector space over E under addition and multiplication in F.

Did you observe that vectors in the examples 3, 4 and 5 have neither a magnitude nor a direction that we know of.

Theorem 1: Let V be a vector space over the field F. Then

i). for each $v \in V$, $0 \cdot v = 0$.

ii). for each $v \in V$, $(-1) \cdot v = -v$

iii). for each $\alpha \in F$, $\alpha 0 = 0$.

iv). for each $\alpha \in F$ and $v \in V$, if $\alpha \neq 0$ and $\alpha v = 0$, then $v = 0$.

Proof:

i). It should be clear to you that the zero in the left hand side of $0v = 0$ is the zero in F and that in the right hand side is the vector zero.

Let $v \in V$. Because $0 = 0 + 0$, where $0 \in F$, $0 \cdot v = (0+0) \cdot v = 0v + 0 \cdot v$.

Because $0 \cdot v \in V$ and V is a vector space, there exists $-(0 \cdot v) \in V$ such that $0 \cdot v + (-(0 \cdot v)) = 0$. Now, $0 = 0 \cdot v + (-(0 \cdot v)) = (0 \cdot v + 0 \cdot v) + (-(0 \cdot v))$

$= 0 \cdot v + (0 \cdot v + (-(0 \cdot v))) = 0 \cdot v + 0 = 0 \cdot v$. That is, $0 \cdot v = 0$.

ii). Let $v \in V$. Observe that $v + (-1)\cdot v = 1\cdot v + (-1)\cdot v = (1+(-1))\cdot v = 0\cdot v = 0$. By the uniqueness of the additive inverse (see proposition 1 on page 11), $-v = (-1)\cdot v$.

iii). Again, it should be clear to you that the zero in $\alpha \cdot 0 = 0$ is the vector zero.

To prove this, let $\alpha \in F$. Note that $\alpha\cdot 0 = \alpha\cdot(0+0) = \alpha\cdot 0 + \alpha \cdot 0$. Because $\alpha\cdot 0 \in V$ and V is a vector space, there exists $-(\alpha\cdot 0) \in V$ such that $\alpha\cdot 0 + (-(\alpha\cdot 0)) = 0$. So, $0 = \alpha\cdot 0 + (-(\alpha\cdot 0)) =$
$(\alpha\cdot 0 + \alpha\cdot 0) + (-(\alpha\cdot 0)) = \alpha\cdot 0 + (\alpha\cdot 0 + (-(\alpha\cdot 0))) = \alpha\cdot 0 + 0 = \alpha\cdot 0$.
That is, $\alpha\cdot 0 = 0$.

iv). Let $\alpha \in F$ and $v \in V$. Assume $\alpha \neq 0$ and $\alpha v = 0$. Because $\alpha \neq 0$ (0 in F) and F is a field, there exists $\alpha^{-1} \in F$ such that $\alpha\cdot\alpha^{-1} = 1$.
Now, $v = 1\cdot v = (\alpha\cdot\alpha^{-1})\cdot v = (\alpha^{-1}\alpha)\cdot v = \alpha^{-1}(\alpha v) = \alpha^{-1} 0 = 0$. This completes the proof.

Exercise 1: Let V be a vector space over the field F. Prove that for each $u, v \in V$ and $\alpha, \beta \in F$, $\alpha u + \beta v \in V$.

Remark: Because vector addition is commutative and associative, the way in which vectors in a sum are combined and associated is irrelavent. For example if $v_1, v_2, v_3, v_4 \in V$, then
$(v_1+v_2)+(v_3+v_4) = [v_3 + (v_1+v_4)] + v_2$. Thus, such a sum may be written without confusion as $v_1+v_2+v_3+v_4$.

Subspaces:

Definition 4: Let V be a vector space over the field F. A subspace of V is a nonempty subset W of V which is itself a vector space over F under the operations of vector addition and scalar multiplication on V.

Thus, in order to show that $\emptyset \neq W \subseteq V$ is a subspace of the vector space V over F, one must prove that W is closed under vector addition in V, W is closed under scalar multiplication in V, and that W with the two operations satisfy all the 8 axioms of a vector space.

Observe, however, that axiom's (i), (ii), (v), (vi), (vii), and (viii) are valid for W since they are already valid in V. Indeed, these axioms are properties of the operations on V.

Hence, to prove that W is a subspace of V, we must prove that W is closed under $+$ and $\cdot$, $0 \in W$ and for each $w \in W$, $-w \in W$.

If you observed carefully, you will see that this is equivalent to prove that W is closed under $+$ and $\cdot$. We, thus, have the following theorem.

Theorem 2: Let V be a vector space over the field F and W be a nonempty subset of V. Then W is a subspace of V if and only if

a). for each $u, v \in W$, $u+v \in W$ and

b). for each $u \in W$ and $\alpha \in F$, $\alpha u \in W$.

Proof: Suppose W is a subspace of V. Then clearly for each $u, v \in W$ and $\alpha \in F$, $u+v \in W$ and $\alpha u \in W$ as W is itself a vector space over F (so, W is closed under $+$ and $\cdot$).

Conversely suppose that for each $u, v \in W$, $u+v \in W$ and for each $u \in W$ and $\alpha \in F$, $\alpha u \in W$. Let us prove that $0 \in W$ and for each $u \in W$, $-u \in W$. Let $u \in W$ (note that $W \neq \phi$). Then $0 = 0.u \in W$. Now let $u \in W$. Then, $-u = (-1).u \in W$ and $u + (-u) = 0$. The axioms (i), (ii), (v), (vi), (vii), (viii) holds in W as they are properties of the operations on V. Thus W is a subspace of V.

This completes the proof.

One might combine (a) and (b) above to obtain the following equivalent theorem.

Theorem 3: Let V be a vector space over the field F and W be a nonempty subset of V. Then W is a subspace of V if and only if for each $u, v \in W$ and $\alpha \in F$, $\alpha u + v \in W$.

Proof: Exercise.

Examples:

1). If V is a vector space over the field F then V itself is a subspace of V. Also, $W = \{0\}$ - the sub set of V consisting of the zero vector alone - is a subspace of V. W is called the zero subspace of V. Both V and $\{0\}$ are called trivial subspaces.

2). Let F be a field. Then, the set of all n-tuples $u = (x_1, x_2, \ldots, x_n)$ with $x_i = 0$ for some fixed i such that $1 \le i \le n$, is a subspace of F^n under $+$ and $\cdot$ defined as in example 2 on page 13.

3). $W = \left\{ \begin{bmatrix} a & b \\ b & d \end{bmatrix} \;\middle|\; a, b, d \in \mathbb{R} \right\}$ is a subspace of

$V = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{R} \right\}$ under usual addition and scalar multiplication of matrices.

4). In $\mathbb{R}^2$, any line passing through the origin is a subspace of $\mathbb{R}^2$. Can you think of any other non-trivial subspace of $\mathbb{R}^2$ other than lines passing through the origin?

5). In $\mathbb{R}^3$, any line passing through the origin is a subspace of $\mathbb{R}^3$. Also, any plane passing through the origin is a subspace of $\mathbb{R}^3$.
Can you think of any other non-trivial subspace of $\mathbb{R}^3$ other than lines and planes passing through the origin?

Definition 5: Let V be a vector space over the field F and let $v_1, v_2, \ldots, v_n \in V$. A linear combination of $v_1, v_2, \ldots, v_n$ is a sum of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where $\alpha_i \in F$ for each $i = 1, 2, \ldots, n$.

If $u \in V$ and $u = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ for some $v_i \in V$ and $\alpha_i \in F$ for each $i = 1, 2, \ldots, n$, then u is said to be a linear combination of the vectors $v_1, v_2, \ldots, v_n$.

Example: Consider the Euclidean space $\mathbb{R}^2$. Then, $3\cdot(2,1) + 5\cdot(0,1) = (6,3) + (0,5) = (6,8)$ is a linear combination of $(2,1)$ and $(0,1)$. So, we say that $(6,8)$ is a linear combination of $(2,1)$ and $(0,1)$. Also $(6,8)$ is a linear combination of $(2,1)$, $(0,1)$ and $(4,6)$ as $(6,8) = 1\cdot(2,1) + 1\cdot(0,1) + 1\cdot(4,6)$.

Theorem 4: Let V be a vector space over the field F and let $S = \{v_1, v_2, \ldots, v_n\} \subseteq V$. Then the set

$$W = \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \mid \alpha_i \in F \text{ for each } i = 1, 2, \ldots, n\}$$

of all linear combinations of vectors in S is a subspace of V such that $v_i \in W$ for each $i = 1, 2, \ldots, n$ and if U is a subspace of V such that $S \subseteq U$, then $W \subseteq U$.

Proof: Because $0 = 0.v_1 + 0.v_2 + \cdots + 0.v_n \in W$, $W \neq \emptyset$. Clearly $W \subseteq V$. Let $u, v \in W$ and $\alpha \in F$. Since $u, v \in W$, there exist

$\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n \in F$ such that

$u = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ and $v = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n$. Note that

$\alpha u + v = \alpha(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) + (\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n) =$

$[(\alpha\alpha_1)\cdot v_1 + (\alpha\alpha_2)\cdot v_2 + \cdots + (\alpha\alpha_n)\cdot v_n] + (\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n) =$

$(\alpha\alpha_1 + \beta_1)\cdot v_1 + (\alpha\alpha_2 + \beta_2)\cdot v_2 + \cdots + (\alpha\alpha_n + \beta_n)\cdot v_n \in W$ as $\alpha\alpha_i + \beta_i \in F$ for each $i = 1, 2, \ldots, n$. Thus, W is a subspace of V.

Now let $i_0 \in \{1, 2, \ldots, n\}$. Note that $v_{i_0} = \sum_{i=1}^{n} \alpha_i v_i$, where for each $i \in \{1, 2, \ldots, n\}$, $\alpha_i = 0$ if $i \neq i_0$ and $\alpha_i = 1$ if $i = i_0$. Thus, $v_{i_0} \in W$.

Hence, $S \subseteq W$.

Finally, suppose that U is a subspace of V containing S. Then clearly $W \subseteq U$ as U is closed under addition and scalar multiplication.

This completes the proof.

Now let $\phi \neq S \subseteq V$, where V is a vector space. Clearly, S does not need to be finite. In such a case, i.e. if S is infinite, we cannot take or form a linear combination of all the vectors in S as we cannot add infinite number of vectors. However, we can consider all the finite linear combinations of vectors in S. This leads to a more general result which covers all the subsets S in V not necessarily finite as is S in Theorem 4 above.

Theorem 5: Let V be a vector space over the field F and let $S \neq \phi$ be a subset of V. Then the set $W = \{\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n \mid n \in \mathbb{N}, v_i \in S$ and $\alpha_i \in F$ for each $i = 1, 2, \dots, n\}$ of all the finite linear combinations of vectors in S is a subspace of V such that $S \subseteq W$ and for each subspace U of V, if $S \subseteq U$, then $W \subseteq U$.

Proof: Exercise.

Definition 6: Let V be a vector space and let $v_1, v_2, \dots, v_n \in V$. Let $S = \{v_1, v_2, \dots, v_n\}$. Then $\text{span}(S)$ is defined as the set of all linear combinations of vectors in S.

That is, $\text{span}(S) = \{\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n \mid \alpha_i \in F$ for each $i = 1, 2, \dots, n$, $v_i \in S$ for each $i = 1, 2, \dots, n\}$

In general, for any $\phi \neq S \subseteq V$, $\text{span}(S)$ is defined as the set of all finite linear combinations of vectors in S. That is, $\text{span}(S) = \{\alpha_1 v_1 + \dots + \alpha_n v_n \mid n \in \mathbb{Z}^+, v_i \in S \text{ and } \alpha_i \in F \text{ for each } i = 1, 2, \dots, n\}$.

• Note that span(S) is a subspace of V.

Definition 7: Let V be a vector space over the field F and let $S \neq \emptyset$ be a subset of V. Then span(S) - generated by forming all the finite linear combinations of vectors in S - is called the "subspace spanned by S".

When S is a finite set of vectors, $S = \{v_1, v_2, \dots, v_n\}$, we shall simply call span (S) the subspace spanned by the vectors $v_1, v_2, \dots, v_n$.

If $V = \text{span}(S)$ for some $S \subseteq V$, We say that S is a spanning set for V. In other words S spans V if each vector in V is a linear combination (or finite linear combination) of vectors in S.

Example: Let $V = \{ f: \mathbb{R} \to \mathbb{R} \mid f \text{ is a polynomial over } \mathbb{R} \}$.

Then, V is a vector space over $\mathbb{R}$ under usual addition and scalar multiplication of functions. Let $S = \{x, x^2, x^3\}$. Clearly $S \subseteq V$. Note that $x^4 + 1 \in V$ and x^4+1 cannot be written as a linear combination of vectors in S. The reason is for any $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, $\alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3$ is a polynomial of degree at most 3. However, x^4+1 is a polynomial of degree 4.

Example: Show that $S = \{ (1,2), (2,1) \}$ spans $\mathbb{R}^2$.

Solution: Clearly $S \subseteq \mathbb{R}^2$. We need to show that $\text{span}(S) = \mathbb{R}^2$.

It is easy to see that $\text{span}(S) \subseteq \mathbb{R}$. Let's prove that $\mathbb{R}^2 \subseteq \text{span}(S)$. To this end, let $(x,y) \in \mathbb{R}^2$. Note that

$\frac{-x+2y}{3}, \frac{2x-y}{3} \in \mathbb{R}$ and $\left(\frac{-x+2y}{3}\right)\cdot(1,2) + \left(\frac{2x-y}{3}\right)\cdot(2,1) =$

$$\left[\frac{-x+2y}{3} + 2\left(\frac{2x-y}{3}\right), 2\left(\frac{-x+2y}{3}\right) + \frac{2x-y}{3}\right] = \left(\frac{-x+4x+2y-2y}{3}, \frac{-2x+2x+4y-y}{3}\right)$$

$= (x, y)$.

Thus, every $(x,y) \in \mathbb{R}^2$ is a linear combination of $(1,2)$ and $(2,1)$. That is $\mathbb{R}^2 \subseteq \text{span}(S)$. Hence $\mathbb{R}^2 = \text{span}(S)$. That is S spans $\mathbb{R}^2$.

Example: Let $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$. Prove that $S = \{e_1, e_2, e_3\}$ spans $\mathbb{R}^3$.

Solution: Clearly $S \neq \phi$ and $S \subseteq \mathbb{R}^3$. It is easy to see that $\text{span}(S) \subseteq \mathbb{R}^3$. We need to show that $\mathbb{R}^3 \subseteq \text{span}(S)$.

So let $(x, y, z) \in \mathbb{R}^3$. Note that $x, y, z \in \mathbb{R}$ and

$$(x, y, z) = x\cdot(1, 0, 0) + y\cdot(0, 1, 0) + z\cdot(0, 0, 1) = x\cdot e_1 + y\cdot e_2 + z\cdot e_3.$$

Thus, (x, y, z) is a linear combination of $(1, 0, 0), (0, 1, 0), (0, 0, 1)$. That is $\mathbb{R}^3 \subseteq \text{span}(S)$. So, $\mathbb{R}^3 = \text{span}(S)$. That is $S = \{e_1, e_2, e_3\}$ spans $\mathbb{R}^3$.

Example: Let $V = \{f : \mathbb{R} \to \mathbb{R}\}$ - the set of all real valued functions on $\mathbb{R}$. Recall that V is a vector space over $\mathbb{R}$ under usual addition and scalar multiplication of functions. Let $S = \{x^n \mid n \in \mathbb{Z}^+ \cup \{0\}\}$. Then, $\text{span}(S)$ (or the subspace spanned by S) is the subspace of all polynomial functions from $\mathbb{R}$ to $\mathbb{R}$.

Example: Let $S = \{(1,0,1), (1,1,0)\}$. Prove that S does not span $\mathbb{R}^3$.

Solution: To the contrary assume that S spans $\mathbb{R}^3$. Then, there exists $x, y \in \mathbb{R}$ such that $x\cdot(1,0,1) + y\cdot(1,1,0) = (0,1,0)$.

So, $x + y = 0$
$y = 1$ and
$x = 0$.

It follows that $1 = 0 + 1 = 0$. This is a contradiction. Thus for each $x, y \in \mathbb{R}$, $x\cdot(1,0,1) + y\cdot(1,1,0) \neq (0,1,0)$. Hence S does not span $\mathbb{R}^3$. In other words $\text{span}(S) \neq \mathbb{R}^3$.

Theorem 6: Let V be a vector space over the field F and let W_1, W_2 be two subspaces of V. Then $W_1 \cap W_2$ is a subspace of V.

Proof: Because $0 \in W_1$ and $0 \in W_2$, $0 \in W_1 \cap W_2$. Thus $W_1 \cap W_2 \neq \emptyset$. Also, because $W_1, W_2 \subseteq V$, $W_1 \cap W_2 \subseteq V$. Now let $u, v \in W_1 \cap W_2$ and $\alpha \in F$. Note that $u, v \in W_1$ and $u, v \in W_2$. Because W_1 is a subspace of V, $\alpha u + v \in W_1$. Because W_2 is a subspace of V, $\alpha u + v \in W_2$. Thus, $\alpha u + v \in W_1 \cap W_2$. Therefore, $W_1 \cap W_2$ is a subspace of V.

The above theorem shows that the intersection of two subspaces of a vector space is also a subspace of V. What can you say about the intersection of any non-empty collection of subspaces of a vector space V? Will it be also a subspace of V? The following theorem shows that it is indeed the case.

Theorem 7: Let V be a vector space over the field F. Then the intersection of any non-empty collection of subspaces of V is a subspace of V.

Proof: Let $\{W_i \mid i \in \Lambda\}$, where Λ is an arbitrary index set, be an arbitrary non empty collection of subspaces of V. Observe that because $0 \in W_i$ for each $i \in \Lambda$, $0 \in \bigcap_{i \in \Lambda} W_i$. Thus, $\bigcap_{i \in \Lambda} W_i \neq \phi$. Since $\bigcap_{i \in \Lambda} W_i \subseteq W_{i_0}$, where $i_0 \in \Lambda$ and $W_{i_0} \subseteq V$, $\bigcap_{i \in \Lambda} W_i \subseteq V$. Now let $u, v \in \bigcap_{i \in \Lambda} W_i$ and $\alpha \in F$. Then $u, v \in W_i$ for each $i \in \Lambda$. Because W_i is a subspace of V for each $i \in \Lambda$, $\alpha u + v \in W_i$ for each $i \in \Lambda$. Thus, $\alpha u + v \in \bigcap_{i \in \Lambda} W_i$. Therefore, $\bigcap_{i \in \Lambda} W_i$ is a subspace of V.

Scanned with CamScanner

Theorem 8: Let V be a vector space over the field F and let S be a non empty subset of V. Then

$$\bigcap_{\substack{W \text{ is a subspace} \\ \text{of } V \text{ and} \\ S \subseteq W}} W = \left\{ \sum_{i=1}^{n} \alpha_i v_i \;\middle|\; \alpha_i \in F \text{ for each } i=1,\dots,n,\ v_i \in S \text{ for each } i=1,\dots,n \text{ and } n \in \mathbb{Z}^+ \right\}$$

$= \text{span}(S)$.

Proof: Observe first that $\{W \mid W \text{ is a subspace of } V \text{ and } S \subseteq W\} \neq \emptyset$ as $V \in \{W \mid W \text{ is a subspace of } V \text{ and } S \subseteq W\}$.

Now let $u \in \text{span}(S)$ and let W be a subspace of V such that $S \subseteq W$. Since $u \in \text{span}(S)$, $u = \sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$ and $v_i \in S$, where $i = 1, 2, 3, \dots, n$. Because W is a subspace and $S \subseteq W$, $v_i \in W$ for each $i \in \{1, \dots, n\}$ and $u = \sum_{i=1}^{n} \alpha_i v_i \in W$. It follows that $u \in \bigcap_{\substack{W \text{ is a subspace} \\ \text{of } V \text{ and} \\ S \subseteq W}} W$. Thus, $\text{span}(S) \subseteq \bigcap_{\substack{W \text{ is a subspace} \\ \text{of } V \text{ and } S \subseteq W}} W$.

Because $S \subseteq \text{span}(S)$ and $\text{span}(S)$ is a subspace, $\text{span}(S) \in \{W \mid W \text{ is a subspace of } V \text{ and } S \subseteq W\}$. Thus,

$$\bigcap_{\substack{W \text{ is a subspace} \\ \text{of } V \text{ and } S \subseteq W}} W \subseteq \text{span}(S).$$

This completes the proof.

Remark: Because $\bigcap_{\substack{W \text{ is a subspace} \\ \text{of } V \text{ and } S \subseteq W}} W = \text{span}(S)$, where S is a nonempty subset of the vector space V, some authors define span(S) (or the subspace spanned by S) to be the intersection of all subspaces of V which contains S. Indeed, for any $S \subseteq V$, they define span(S) to be the intersection of all subspaces of V which contains S. The advantage of this definition of span(S) is that it allows S to be the empty set.

Linear Independence – Linear Dependence.

Definition 8: Let V be a vector space over the field F and let $S = \{v_1, v_2, \dots, v_n\}$ be a subset of V. S is said to be linearly independent (or sometimes we say that $v_1, v_2, \dots, v_n$ are linearly independent instead of saying S is linearly independent) if the only solution for the scalars $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ in the equation $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$ is the trivial solution $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.

S is said to be linearly dependent (or sometimes we say that $v_1, v_2, \dots, v_n$ are linearly dependent instead of saying S is linearly dependent) if S is not linearly independent. In other words, S is linearly dependent if there is a non-trivial solution for the scalars $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ in the vector equation $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$. That is if there exist scalars $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ not all of them 0, such that $\alpha_1 v_1 + \dots + \alpha_n v_n = 0$.

Above, the linear independence (or dependence) of a set was defined when that set is finite. What follows is a more general definition.

Definition 9: Let V be a vector space over the field F and let S be a subset of V. S is said to be linearly independent if $S = \phi$ or $S \neq \phi$ and every non-empty finite subset of S is linearly independent. Thus a non-empty set $S \subseteq V$ is linearly dependent if there exists a non-empty finite subset of S which is linearly dependent.

Remark:
- Any set which contains a linearly dependent set is linearly dependent.
- Any subset of a linearly independent set is linearly independent.
- Any set which contains the 0 (zero) vector is linearly dependent, because $1 \cdot 0 = 0$.

Scanned with CamScanner

Examples:

1). In $\mathbb{R}^3$, $\{(1,0,0), (0,1,0), (0,0,1)\}$ is a linearly independent set. To verify this we must show that the equation

$\alpha_1 \cdot (1,0,0) + \alpha_2 \cdot (0,1,0) + \alpha_3 \cdot (0,0,1) = 0$ has only the trivial solution.

Suppose $\alpha_1 \cdot (1,0,0) + \alpha_2 \cdot (0,1,0) + \alpha_3 \cdot (0,0,1) = 0$. Then $(\alpha_1, \alpha_2, \alpha_3) = 0$.

Note that $0 = (0,0,0)$. So, $(\alpha_1, \alpha_2, \alpha_3) = (0,0,0)$. We know that two vectors $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{R}^n$ are equal if and only if $\alpha_i = \beta_i$ for each $i = 1, 2, \ldots, n$. Because $(\alpha_1, \alpha_2, \alpha_3) = (0,0,0)$, it follows that $\alpha_1 = \alpha_2 = \alpha_3$. That is, the vector equation

$\alpha_1 \cdot (1,0,0) + \alpha_2 \cdot (0,1,0) + \alpha_3 \cdot (0,0,1) = 0$ has only the trivial solution.

Thus, $\{(1,0,0), (0,1,0), (0,0,1)\}$ is linearly independent.

2). In $\mathbb{R}^2$, $\{(1,2), (3,5), (7,11)\}$ is linearly dependent because

$(-2) \cdot (1,2) + 3 \cdot (3,5) + (-1) \cdot (7,11) = (0,0)$ and not all the scalars -2, 3 and -1 are 0.

Exercise: Determine whether the set $\{(1,-1,5), (2,1,2), (-2,-10,22)\}$ in $\mathbb{R}^3$ is linearly independent or not.

Solution: We need to check whether the equation

$$\alpha_1(1,-1,5) + \alpha_2 \cdot (2,1,2) + \alpha_3 \cdot (-2,-10,22) = (0,0,0)$$ has

only the trivial solution or not. Let us solve the

system of linear equations:

$$\alpha_1 + 2\alpha_2 - 2\alpha_3 = 0 \quad — (1)$$

$$-\alpha_1 + \alpha_2 - 10\alpha_3 = 0 \quad — (2)$$

$$5\alpha_1 + 2\alpha_2 + 22\alpha_3 = 0. \quad — (3)$$

(1) + (2) gives $3\alpha_2 - 12\alpha_3 = 0$ which is equivalent to

$$\alpha_2 - 4\alpha_3 = 0. \quad — (2)'$$

$(-5).(1) + (3)$ gives $-8\alpha_2 + 32\alpha_3 = 0$ which is equivalent to

$$\alpha_2 - 4\alpha_3 = 0 \quad — (3)'.$$

Thus, the reduced system of linear equations is,

$$\alpha_1 + 2\alpha_2 - 2\alpha_3 = 0 \quad — (1)$$

$$\alpha_2 - 4\alpha_3 = 0 \quad — (2)'.$$

Now, we have 3 variables and only two equations. Thus, we let α_1 to be a free variable. So let $\alpha_1 = t$, where $t \in \mathbb{R}$. Then,

$$2\alpha_2 - 2\alpha_3 = -t \quad — (1)' \quad \text{and}$$

$$\alpha_2 - 4\alpha_3 = 0 \quad — (2)'.$$

Let us solve (1)' and (2)' in terms of t.

①' + (−2)·②' gives $6\alpha_3 = -t$. Thus, $\alpha_3 = -t/6$. By back substitution in ①': $2\alpha_2 - 2(-t)/6 = -t$ and hence $\alpha_2 = -2/3\, t$.

So, $\alpha_1 = t$, $\alpha_2 = -2/3 \cdot t$ and $\alpha_3 = -1/6 \cdot t$. When t takes different values, we get different solutions for our system of linear equations. We let $t = 6$. Then $\alpha_1 = 6$, $\alpha_2 = -4$ and $\alpha_3 = -1$.

Thus, the vector equation $\alpha_1 \cdot (1,-1,5) + \alpha_2 \cdot (2,1,2) + \alpha_3 \cdot (-2,-10,22) = (0,0,0)$ has a non-trivial solution namely $\alpha_1 = 6$, $\alpha_2 = -4$ and $\alpha_3 = -1$.

Indeed, observe that $6(1,-1,5) + (-4)\cdot(2,1,2) + (-1)\cdot(-2,-10,22) = (6,-6,30) + (-8,-4,-8) + (2,10,-22) = (6-8+2, -6-4+10, 30-8-22) = (0,0,0)$. Therefore, $\{(1,-1,5), (2,1,2), (-2,-10,22)\}$ is linearly dependent. In other words $\{(1,-1,5), (2,1,2), (-2,-10,22)\}$ is not linearly independent.

Exercise: Consider the vector space V of all the polynomials (over $\mathbb{R}$) over the field $\mathbb{R}$. Let $n \in \mathbb{N}$. Determine whether the set $\{1, x, x^2, \ldots, x^n\}$ is linearly dependent or not. (tutorial problem)

Note: Let V be a vector space over the field F.

If $\alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n = 0$ for some distinct vectors $v_i \in V$ and scalars $\alpha_i \in F$ not all of which are 0 (that is at least one of $\alpha_1, \alpha_2, \ldots, \alpha_n$ is non-zero), then $\alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n = 0$ is called a "linear dependence relation" among $v_1, v_2, \ldots, v_n$.

Exercise: Let V be a vector space over the field F and let S be a nonempty subset of V. Let $u \in S$. Prove that if u can be written as a linear combination of some other vectors (finite) in S, then

$$\text{span}(S) = \text{span}(S \setminus \{u\}).$$ (Tutorial problem).

Lemma 1: Let $V \neq \{0\}$ be a vector space over the field F and let $S = \{v_1, v_2, \dots, v_n\}$ be a linearly independent subset of V. Then every element in span(S) has a unique representation in the form $\alpha_1 v_1 + \dots + \alpha_n v_n$ with $\alpha_i \in F$ for $i = 1, 2, \dots, n$.

Proof: Let $u \in$ span(S). Then, by definition, $u = \alpha_1 v_1 + \dots + \alpha_n v_n$ for some $\alpha_1, \dots, \alpha_n \in F$. To show uniqueness, assume $u = \beta_1 v_1 + \dots + \beta_n v_n$ for some other $\beta_1, \dots, \beta_n \in F$ as well. Then, $\alpha_1 v_1 + \dots + \alpha_n v_n = \beta_1 v_1 + \dots + \beta_n v_n$. It follows that $(\alpha_1 - \beta_1) \cdot v_1 + \dots + (\alpha_n - \beta_n) \cdot v_n = 0$. Thus by the linear independence of S, $\alpha_i - \beta_i = 0$ for each $i = 1, 2, \dots, n$. That is, for each $i = 1, 2, \dots, n$, $\alpha_i = \beta_i$. Thus we have the uniqueness.

Theorem 9: Let $V \neq \{0\}$ be a vector space over the field F and let $S = \{v_1, v_2, \dots, v_n\}$ be a set of non-zero vectors in V. Then, S is linearly independent or there exist $v_k \in S$, with $k > 1$, such that v_k is a linear combination of the preceding vectors $v_1, \dots, v_{k-1}$.

Proof: If S is linearly independent, then there is nothing to prove. So, assume S is not linearly independent. Then, S is linearly dependent. Thus there exist $\alpha_1, \ldots, \alpha_n \in F$, not all of which are 0, such that $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$. Let k be the largest integer for which $\alpha_k \neq 0$. To the contrary assume that $k = 1$. Then $\alpha_i = 0$ for each $i = 2, \ldots, n$. That is $\alpha_1 v_1 = 0$. This implies that $v_1 = 1 \cdot v_1 = (\alpha_1^{-1} \alpha_1) \cdot v_1 = \alpha_1^{-1} (\alpha_1 v_1)$ $= \alpha_1^{-1} \cdot 0 = 0$, which is a contradiction as v_1 (indeed all of the vectors in S) is non-zero. Thus $k > 1$.

Now, $\alpha_i = 0$ for each $n \geq i > k$. Hence $\alpha_1 v_1 + \cdots + \alpha_{k-1} v_{k-1} + \alpha_k v_k = 0$. Since $\alpha_k \neq 0$, it implies that $v_k = \alpha_k^{-1} (-\alpha_1 v_1 - \cdots - \alpha_{k-1} v_{k-1}) =$ $(-\alpha_k^{-1} \alpha_1) v_1 + \cdots + (-\alpha_k^{-1} \alpha_{k-1}) v_{k-1}$. Thus, v_k is a linear combination of the preceding vectors $v_1, \ldots, v_{k-1}$. This completes the proof.

Corollary 1: Let $V \neq \{0\}$ be a vector space over the field F and let $S = \{v_1, v_2, \ldots, v_n\} \subseteq V$. If span$(S) = W$ and $\{v_1, \ldots, v_k\}$ is linearly independent, then there exists a linearly independent subset T of S such that $\{v_1, \ldots, v_k\} \subseteq T$ and span$(T) = W$.

Proof: Suppose span $(S) = W$ and $\{v_1, \ldots, v_k\}$ is linearly independent. If $k = n$, that is if S is linearly independent, then we are done. Suppose S is not linearly independent. That is, suppose S is linearly dependent. WLOG assume $v_i \neq 0$ for each $i \in \{1, \ldots, n\}$. For if $v_{i_0} = 0$ for some $i_0 \in \{1, \ldots, n\}$, then we let $S = S'$, where $S' = \{v_1, \ldots, v_n\} \setminus \{v_{i_0}\}$, because $\operatorname{span}(\{v_1, \ldots, v_n\}) = \operatorname{span}(\{v_1, \ldots, v_n\} \setminus \{v_{i_0}\})$. Then by Theorem 9, there exists $v_i \in S$ such that v_i is a linear combination of the preceding vectors $v_1, \ldots, v_{i-1}$. Let j be the smallest index for which v_j is a linear combination of the preceding vectors $v_1, \ldots, v_{j-1}$. Now, since $\{v_1, \ldots, v_k\}$ is linearly independent, $j > k$. Let $T_1 = \{v_1, \ldots, v_k, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\}$. Note that $v_j \notin T_1$. Clearly span $(T_1) \subseteq W$. Now suppose $w \in W$. Because span $(S) = W$, there exists $\alpha_1, \ldots, \alpha_n \in F$ such that $\alpha_1 v_1 + \cdots + \alpha_j v_j + \cdots + \alpha_n v_n = w$. Since v_j is a linear combination of the vectors $v_1, \ldots, v_{j-1}$, there exist $\beta_1, \ldots, \beta_{j-1} \in F$ such that $v_j = \beta_1 v_1 + \cdots + \beta_{j-1} v_{j-1}$. Hence

$$w = \alpha_1 v_1 + \cdots + \alpha_j(\beta_1 v_1 + \cdots + \beta_{j-1} v_{j-1}) + \cdots + \alpha_n v_n = (\alpha_1 + \alpha_j \beta_1) v_1 + \cdots + (\alpha_{j-1} + \alpha_j \beta_{j-1}) v_{j-1}$$
$$+ \alpha_{j+1} v_{j+1} + \cdots + \alpha_n v_n.$$

Thus, $w \in \operatorname{span}(T_1)$. Therefore, span $(T_1) = W$.

Now, consider the set T_1. If T_1 is linearly independent, then we are done. Because, if that is the case, $\{v_1, \dots, v_k\} \subseteq T_1$ and $\text{span}(T_1) = W$. Also, $T_1 \subseteq S$. If T_1 is not linearly independent, then we can proceed as above to obtain a new proper subset T_2 of T_1 such that $\text{span}(T_2) = W$.

Continuing this process, we finally reach a subset $T = \{v_1, \dots, v_k, v_{i_1}, \dots v_{i_r}\}$ of S whose span is still W (i.e. $\text{span}(T) = W$) but in which no element is a linear combination of the preceding vectors. It follows from Theorem 9 that T is not linearly dependent or equivalently T is linearly independent.

This completes the proof.

Corollary 2: Let $V \neq \{0\}$ be a vector space over the field F. If V is spanned by a finite subset of V, then V contains a finite, linearly independent set S such that $\text{span}(S) = V$.

$= \{v_1, \dots, v_n\}$

Proof: Assume that $V = \text{span}(T)$ for some finite set T in V. WLOG assume that T consists of only nonzero vectors. Then by corollary 1, there exists a linearly independent subset S of T such that $\text{span}(S) = V$. Clearly, because T is finite, S is also finite.