Contents

Chapter 1

Fields and Ideals

1.1 Fields

In linear algebra, we are typically analyzing the properties of different vector spaces and linear operators acting on these vector spaces. These vector systems can be defined over a number of different number systems. At this point we should be comfortable with a variety of number systems. We have

1. Real number $\mathbb{R}$
2. Complex number $\mathbb{C}$
3. Rationals $\mathbb{Q}$
4. Integers $\mathbb{Z}$
5. Interger mod n $(\mathbb{Z}_n)$ or $GL(n)$

While we might think that we can define vector spaces over all of these number systems, we are not able to use all of them. We can only use number systems with "nice" properties. The vector spaces are defined over fields.

Definition.

A field , denoted $\mathbb{F}$, is a set which has two binary operators

$$+_{\mathbb{F}} \ (addition) \ and \ \times_{\mathbb{F}}$$

multiplication such that if $a, b \in \mathbb{F}$, then

(a) $a +_F b \in F$

(b) $a \times_F b \in F$

The set must satisfy the following rules:

1. The additive identity exists (0_F).
   $\exists\ 0_F$ s.t. $0_F +_F a = a_F \quad \forall a \in F$

2. The additive inverse exists.
   $\exists\ b$ s.t. $b +_F a = 0 \ \forall a \in F$ (denoted $b = -a$)

3. Associative with addition. $a +_F (b +_F c) = (a +_F b) +_F c$, $\forall a, b, c \in F$

4. Commutative with addition $a +_F b = b +_F a$, $\forall a, b \in F$

5. The multiplication identity exist (1_F)
   $\exists\ 1_F$ s.t. $1_F \times_F a = a$, $\forall a \in F$

6. The multiplication inverse exist (a^{-1})
   $\exists\ a_F^{-1} \in F$ s.t. $a_F^{-1} \times_F a = 1_F \quad \forall a \neq 0_F; a \in F$

7. Associative with multiplication $a \times_F (b \times_F c) = (a \times_F b) \times_F c$

8. Commutative with multiplication $a \times_F b = b \times_F a$

9. Multiplication distributes over addition $a \times_F (b +_F c) = a \times_F b + a \times_F c$

If we consider $+_F$ and $\times_F$ to be the standard operations that we are accustom to, the let use consider the number systems from before. We can see that for real numbers and complex numbers, we satisfy these conditions.

The integers is where we hit our first snag. We know that $2 \in \mathbb{Z}$, but the multiplicative inverse $\frac{1}{2} \notin \mathbb{Z}$. Therefore, the integers does not form a field with the usual addition and multiplication operators. I should note that, addition and multiplication operators exists such that $\mathbb{Z}$ is a field, but we will not discuss this now.

The rational number do form a field. This is a little less clear and would be worth the exercise to prove to oneself.

Now to consider integers mod n $(\mathbb{Z}_n)$. The idea with integers mod n, that that you apply the addition and multiplication operators as you normally would, but after you get your result you subtract or add by factors of n, until you get a number between 0 and $n-1$ inclusive. This can be done using the long division and keeping the remainder.

47 mod 3

$$\begin{array}{r} 15 \\ 3\overline{)47} \\ 3 \\ \hline 17 \\ 15 \\ \hline 2 \end{array} \qquad r = 2$$

If we are looking at $\mathbb{Z}_6$, then

$3+5 = 8 \bmod 6 = 2$ $\qquad$ $3 \times 5 = 15 \bmod 6 = 3$

Note that 5 is acting like the identity operator to 3. It turns our that $\mathbb{Z}_6$ is not a field.

In fact on can show that $\mathbb{Z}_n$ is a field if and only if n is a prime number

We typically define these field to be $\mathbb{Z}_p$. Fields that contain a finite number of elements are called finite fields.

Theorem 1.1.1.

Suppose that $\mathbb{F}$ is a field, with operators $+_{\mathbb{F}}$ and $\times_{\mathbb{F}}$. Then the following are statements are true. (We will prove the first)

1. The additive identity 0_F is unique.
2. The multiplicative identity 1_F is unique.
3. For an $a \in F$, the additive inverse $-a \in F$ is unique.
4. For an $a \in F$, the multiplication inverse a^{-1} is unique.
5. Addition is cancellational; For any $a,b,c \in F$, if $a +_F b = a +_F c$, then $b = c$
6. Given $a \neq 0_F$, multiplication is cancellation; $\forall a,b,c \in F$, if $a \times_F b = a \times_F c$, then $b = c$
7. $0_F \times_F a = a \times_F 0_F = 0_F \ \forall \ a \in F$.
8. Multiplication is distributive over addition. $a \times_F (b +_F c) = a \times_F b + a \times_F c$
9. If $a,b \in F$ and $a \times_F b = 0$, then $a = 0$ or $b = 0$

Proof. Suppose the identity is not unique. Then there exist $\bar{0} \neq \hat{0}$ are both the additive identity. Then by definition $\hat{0} +_{\mathbb{F}} \bar{0} = \hat{0}$. As addition is commutative, $\hat{0} +_{\mathbb{F}} \bar{0} = \bar{0} +_{\mathbb{F}} \hat{0} = \bar{0}$ by definition. Therefore $\bar{0} = \hat{0}$, which is our contradiction. □

Note that to show something is not a field we typically show that one of these statements fail, however prove one of these statements to be true does not prove it is a field

We typically call such conditions necessary, but not sufficient, conditions.

1.2 Rings and Ideals

A ring is a generalization of a field. A ring satisfies the following properties.

Definition.

A set $\mathcal{R}$ is a ring with additive ($+_{\mathcal{R}}$) and multiplicative ($\times_{\mathcal{R}}$) operators such that

(a) If $a,b \in R$, then $a +_R b \in R$

(b) If $a,b \in R$, then $a \times_R b \in R$

1. The additive identity exists (0_R).
   $\exists\ 0_R$ s.t. $0_R +_R a = a \quad \forall a \in R$
2. The additive inverse exists.
   $\exists\ b$ s.t. $b +_R a = 0_R\ \forall a \in R$ (denoted $b = -a$)
3. Associative with addition. $a +_R (b +_R c) = (a +_R b) +_R c$, $\forall a,b,c \in R$
4. Commutative with addition $a +_R b = b +_R a$, $\forall a,b \in R$
5. The multiplication identity exist (1_F)
   $\exists\ 1_R$ s.t. $1_R \times_R a = a$, $\forall a \in R$
6. Associative with multiplication $a \times_R (b \times_R c) = (a \times_R b) \times_R c$
7. Multiplication distributes over addition $a \times_R (b +_R c) = a \times_R b + a \times_R c$

This means that a multiplicative inverse does not need to exist and multiplication is not necessarily commutative. Note that by definition all field are rings. If you take an abstract algebra class you will spend much more time looking into rings. We will spend limited time looking at rings. We introduce them here so that we can define an ideal.

Definition.

Let $(R,+,\times)$ be a ring, let $(R,+)$ be its additive group, then a subgroup I of the additive group $(\mathcal{R},+)$ is a left ideal (right ideal) if $\forall r \in R$ if $x \in I$,then $rx \in I$. An ideal that is left and right sided is called a two-sided ideal.

From the commutative property of multiplications, all ideals of a field are two sided.

Example 1.1.

1. Even numbers form an ideal within the integer
2. Real nxn matrix form an ideal

Definition.

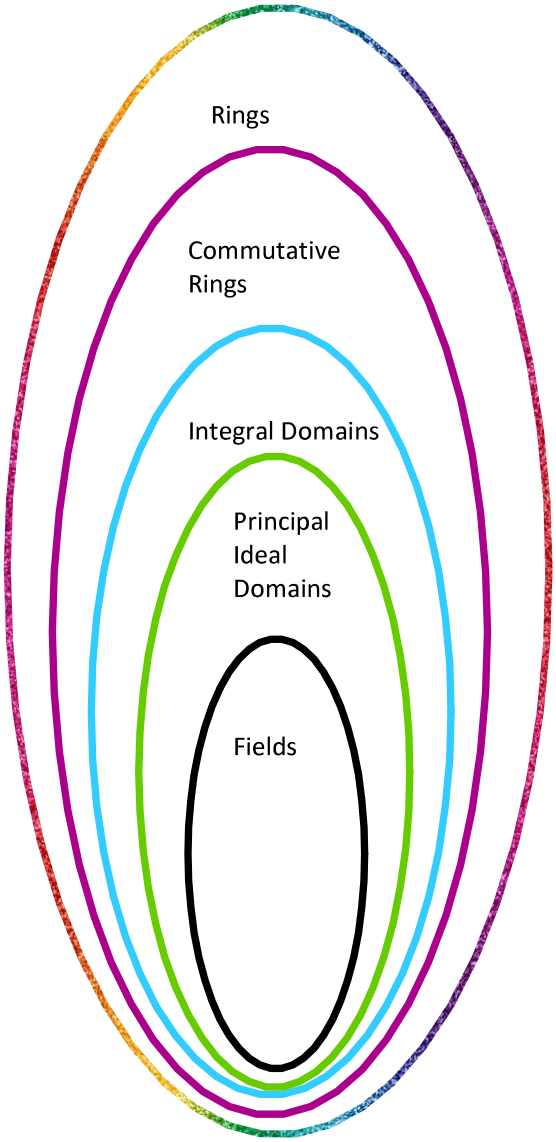
A integral domain Id is a commutative non-zero ideal satisfies the condition that if $a,b \in Id$ and $ab=0$, then $a=0$ or $b=0$ (equivalent to multiplication is cancellation)

Ideals can be generated by a subset of elements within I, by adding these elements together we can generate the entire ideal. An principal ideal is an ideal that can be generated using a single element. Having a basic understanding of ideals and principal ideals is not necessary, but will help later in the course when we discuss polynomial ideals .

A principal ideal domain is a integral domain such that every ideal within the integral domain is a principal ideal.

It is a common mistake to think that by proving something is an integral domain , then we have proven it is a field , however, we can see that the integers are an integral domain , but we have already proven that they are not a field when using the standard multiplication and addition operators.

May 12, 2023 4:12 PM



Rings (R,+,x)
- R - a set
- + - additive operator
- X - multiplication operator

- Close under addition
- Close under multiplication

- Additive identity exists
- Additive inverse exists
- Addition is associative
- Addition is commutative
- Multiplication identity exists
- Multiplication is associative
- Multiplication distributes over addition

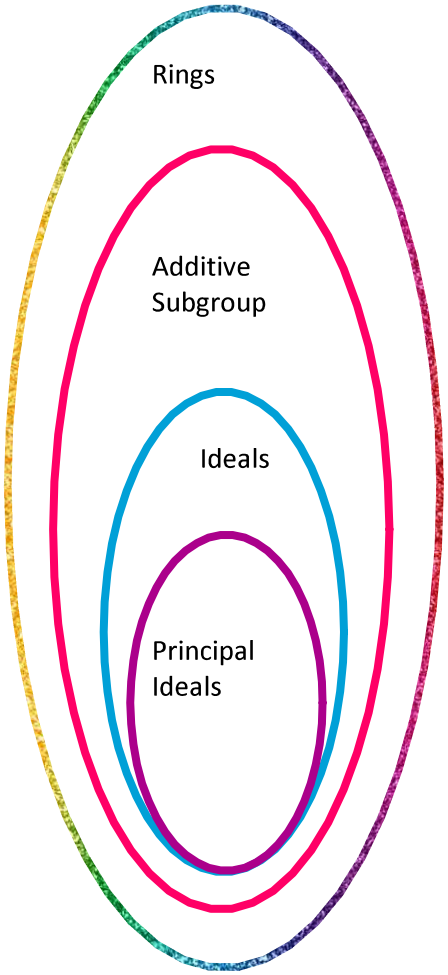
Commutative Rings
- Ring + Multiplication is commutative

Integral Domains
- Commutative Ring + if ab= 0 then a=0 or b=0

Principal Ideal Domains
- Integral Domain + all ideals are principal ideals

Fields
- Principal Ideal Domain + Multiplication inverse exists.

May 12, 2023 4:22 PM



Rings (R,+,x)
- R - a set
- + - additive operator
- X - multiplication operator

- Close under addition
- Close under multiplication

- Additive identity exists
- Additive inverse exists
- Addition is associative
- Addition is commutative
- Multiplication identity exists
- Multiplication is associative
- Multiplication distributes over addition

Additive subgroup (A,+)
- A is a subgroup of R
- + - the additive operator from the ring

- Closed under addition

- Additive identify exists
- Additive inverse exists
- Associative with addition

Ideal
- Additive subgroup (I,+) such that
  - a in I, and r in R, then a*r in I
    - (using the multiplication operator from the ring

Principal ideal
- An ideal that can be generated using a single element

Chapter 2

Vector Spaces

[1] In this chapter we chapter we will review the basics for vector spaces, over a field $\mathbb{F}$. You may or may not have seen this over a general field. Some of you may have only seen this discussed over the real numbers and/or complex number.

[1]The note from this chapter are adapted from notes written by Damien Roy and Pierre Bel, translated to English by Alistair Savage

2.1 Vector Spaces

Definition.

A vector space over a field F is a set V with addition and scalar multiplications operators such that

1. If $a, b \in V$, then $a+b \in V$
2. If $a \in V$ and $c \in F$, then $ca \in F$

If V is a vector space, then V satisfies the following properties. Let $a, b \in \mathbb{F}$ and $u, v \in V$

1. If $w \in V$, then $u+(v+w) = (u+v)+w$
2. $u+v = v+u$
3. $\exists\ \vec{0} \in V$ s.t. $v+\vec{0} = v \quad \forall v \in V$ (zero vector)
4. $\forall v \in V, \exists -v \in V$ s.t. $v+(-v) = 0$ (additive inverse)
5. $1 \times v = v$
6. $a(bv) = (ab)v$
7. $(a+b)v = av+bv$
8. $a(u+v) = au+av$

If $v_1, \ldots, v_n \in V$, $a_1, \ldots, a_n \in F$, then $\left(\sum_{i=1}^{n} a_i v_i\right) \in V$

You have seen that vectors in $\mathbb{R}^n$ are vectors spaces, but there are many other vector spaces that exists.

Example 2.1.

1. The set of polynomials with coefficients in F ($F[x]$)
2. The set of $n \times m$ matrix where the entries are in F.
3. A vector, whose entries are in $\mathbb{Z}_p$.

We will prove that the polynomial with coefficients in $\mathbb{F}$ form a vector space. I would encourage you to prove the others form a vector space.

If $a \in F[x]$, then $a = \sum_{i=0}^{n} a_i x^i$, where $a_i \in F$.
Let $a, b \in F[x]$, without loss of generality we will assume that $n = \text{degree}(a) \geq \deg(b) = m$.
Then $b = \sum_{i=0}^{n} b_i x^i$ where $b_i = 0 \ \forall \ m < i \leq n$.
Then $a + b = \sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i \in F[x]$.

Most of these results follow from V being defined over a field. The properties of the field extend to the vector space.

2.2 Vector Subspaces

Definition.

A vector subspace of V is a subset U of V satisfying the following conditions:

1. $0 \in U$
2. if $a, b \in U$, then $a+b \in U$
3. if $a \in U$ and $c \in F$, then $ca \in U$

For each of these propositions, convince yourself that they are correct.

Proposition 2.2.1.

Let U be a non-empty subset of V. Then the set U is a subspace of V over the field $\mathbb{F}$ if

1. if $a, b \in U$, then $a+b \in U$
2. if $a \in U$ and $c \in F$, then $ca \in U$

This is what is meant when we say that addition and scalar multiplication is restricted *from* V *to* U .

Proposition 2.2.2.

If U is a subspace of V and W is a subspace of U, then W is a subspace of V.

When dealing with sets we are use to looking at the union and intersection of the sets. For vector spaces we will look at the sum and intersection of subspaces.

Proposition 2.2.3.

Let $U_1, \cdots, U_n$ be a collection of subspaces of V, then the sum of the subspaces and the intersection of the subspaces are subspaces of V.

Sum : $U_1 + \cdots + U_n = \{u_1 + \cdots + u_n ; u_1 \in U_1, \cdots, u_n \in U_n\}$.

Intersection : $U_1 \cap \cdots \cap U_n = \{u ; u \in U_1, \cdots, u \in U_n\}$.

2.3 Bases

Definition.

An element $v \in V$ is a linear combination of $v_1, \cdots, v_n$ if there exists $a_1, \cdots, a_n \in \mathbb{F}$ such that

$$v = a_1 v_1 + \cdots + a_n v_n.$$

Definition.

The span of as a set of vectors $v_1 + \cdots + v_n \in V$ is the set of all vectors in V that can be made using a linear combination of vectors in V.

$$\text{span}\{v_1, \cdots, v_n\} = \{a_1 v_1, a_2 v_2, \ldots, a_n v_n\}$$

In some cases, $span_{\mathbb{F}}$ will be used to remind the reader, the field on which the vector space is defined over.

Proposition 2.3.1.

Let V be a vector space and $v_1, \cdots, v_n \in V$. Then the span$\{v_1, \cdots, v_n\}$ is a subspace of V and is contained in all the subspaces of V that contain $v_1, \cdots, v_n$.

Definition.

If the span{v1,...,vn} = V , we say that the set {v1,...,vn} generates the vector space V.

Remember that $\{v_1, \cdots, v_k\}$ is a set of vectors, whereas $span\{v_1, \cdots, v_k\}$ is the set of all linear combinations of $\{v_1, \cdots, v_k\}$. They are different.

Definition.

A set of vectors $v_1, \cdots, v_k \in V$ are linearly independent if

$$a_1 v_1 + \cdots + a_n v_n = 0 \iff a_1 = \cdots = a_n = 0$$

This is equivalent to saying that for any $v_i \notin \{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k\}$. If $v_i \in span\{v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k\}$, then the vectors $v_1, \cdots, v_k$ are linearly dependent

Definition.

A set $\{v_1, \cdots, v_k\}$ is a basis of V if $\{v_1, \cdots, v_k\}$ is a set of linear independent vectors that generates V.

Proposition 2.3.2.

Suppose the $\{v_1, \cdots, v_k\}$ is a basis for V. Then for all $v \in V$ a unique choice of scalars $a_1, \cdots, a_k \in \mathbb{F}$ exists such that

$$v = a_1 v_n + \cdots + a_n v_n$$

Definition.

If $\beta = \{v_1, \vdots, v_n\}$ is a basis for V, the scalars $a_1, \cdots, a_n$ that satisfy $v = a_1 v_n + \cdots + a_n v_n$ are called the coordinates of v in the basis β. The coordinate vector is denoted

$$[v]_\beta = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in F^n$$

Example 2.2.

The vectors following vectors form a basis for the vector space $\mathbb{F}^n$.

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \cdots \quad e_n = \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$$

Note that

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n$$

Therefore

$$\therefore \left[\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right]_\beta = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \forall \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in F^n$$

Proposition 2.3.3.

Suppose V is a finite vector space. Then

(a) V has a bases and all bases of V have the same carnality

(b) Every generating set of V contains a bases of V.

(c) Every linear independent set of elements of V is contained in a basis of V.

(d) Every subspace of V has a basis.

Definition.

The carnality of the basis for a vector space is the dimension of the vector space, denoted $dim(V)$.

↓ the # of vector of basis.

Proposition 2.3.4.

If U_1 and U_2 are finite dimensional subspaces of V, then

$$\dim(U_1+U_2)+\dim(U_1\cap U_2)=\dim(U_1)+\dim(U_2)$$

Example 2.3.

Let $\alpha = (1,1,1,0)^T$, $\beta = (0,1,1,1)^T$, $\gamma = (1,0,0,1)^T$.

We can see that $\alpha, \beta, \gamma \in \mathbb{R}^4$ and $\alpha, \beta, \gamma \in (\mathbb{Z}_2)^4$.

Show that α, β, γ are linearly independent in $\mathbb{R}^4$, but linearly dependent in $(\mathbb{Z}_2)^4$.

In $\mathbb{R}^4$:

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right] \to \left[\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

Therefore $a = 0, b = 0, c = 0$.

In $(\mathbb{I}_2)^4$

$$\begin{aligned} (\alpha + \beta) + \gamma &= ((1,1,1,0)^T + (0,1,1,1)^T) + (1,0,0,1)^T \\ &= (1,0,0,1)^T + (1,0,0,1)^T \\ &= (0,0,0,0)^T. \end{aligned}$$

2.4 Direct Sum

For this section, fix V to be a vector space over $\mathbb{F}$ and $V_1, \cdots, V_n$ to be subspaces of V.

Definition.

The sum $V_1 + \cdots + V_n$ is a direct sum if the only choices of vectors $v_1 \in V_1, v_2 \in V_2, \cdots, v_n \in V_n$ such that

$$v_1 + v_2 + \cdots + v_n = 0$$

is $v_1 = \cdots = v_n = 0$. The direct sum is denoted $V_1 \oplus \cdots \oplus V_n$.

Proposition 2.4.1.

Let V be a finite dimension vector space. Then $V = V_1 \oplus \cdots \oplus V_n$ if and only if

(a) $\dim(V) = \dim(V_1) + \cdots + \dim(V_n)$

(b) $\forall i, j,\ i \neq j,\ V_i \cap V_j = \{0\}$

(c) $V = V_1 + \cdots + V_n$

Proposition 2.4.2.

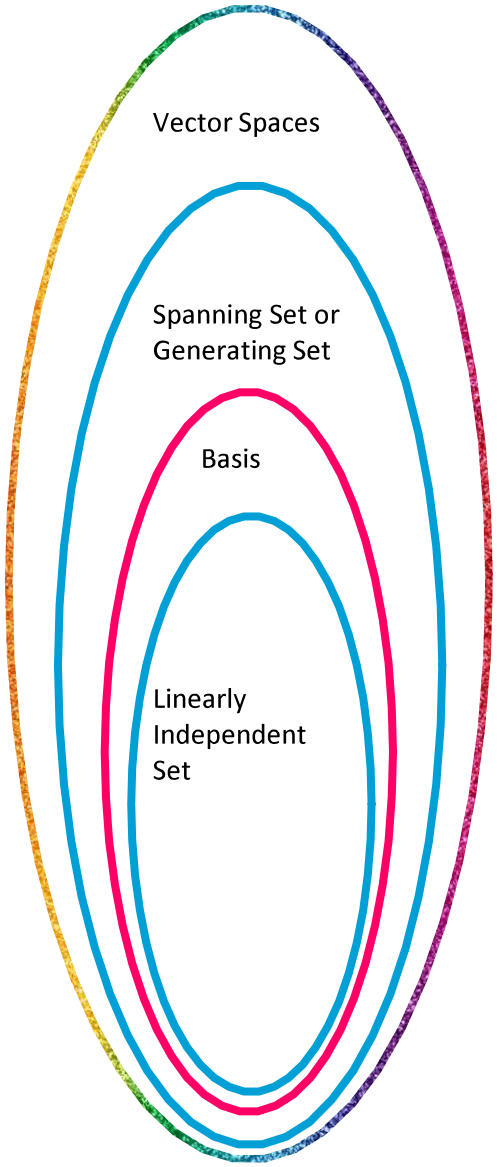
Suppose that $V = V_1 \oplus \cdots \oplus V_n$ *is finite dimensional and* $\beta_i = \{v_{1,1}, \cdots, v_{i,n_i}\}$ *is a basis for all V_i. Then the the* ordered set

$$\beta = \{v_{1,1}, \cdots, v_{1,n_1}, v_{2,1}, \cdots, v_{2,n_2}, \cdots, v_{k,1}, \cdots, v_{k,n_k}\}$$

obtained by concatenating for $\beta_1, \cdots, \beta_k$ *is a basis of V.*

Note that a basis listed in a specific order is called an ordered basis.

May 12, 2023 4:30 PM



Vector Space
Set V over Field F

Closed under addition
Closed under scalar multiplication

such that if a,b in F and u,v,w in V then

u+(v+w) = (u+v)+w
u+v = v+u
Additive identity exists 0 in V s.t. u+0 = u
Additive inverse exists a+ (-a) = 0

Multiplicative identity exist 1 in F s.t. 1*u = 1

a(bu) = (ab)u
(a+b)u = au+bu

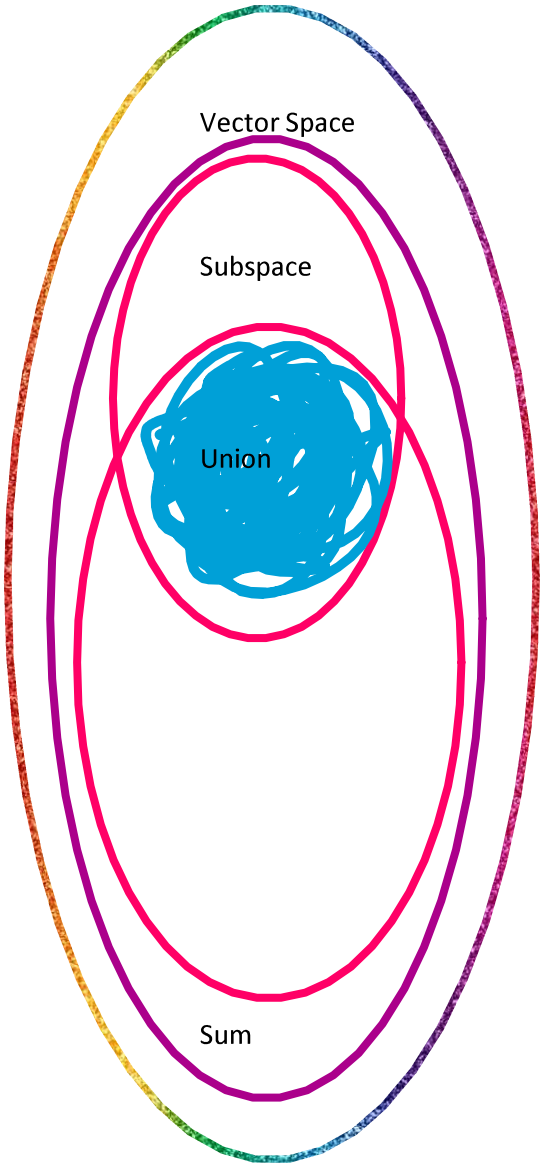
a(u+v) = au + av

Spanning Set or Generative Set (subset of V) (Could be finite)
Subset of V, whose span is equal to V

Basis (subset of a spanning sets) (cardinality = dim(V)
Linearly intendent set that spans the set spans V

Linearly independent set S (cardinality of S <= dim(V))
Subset of a basis

May 12, 2023 4:56 PM



Vector Space
Set V over Field F

Closed under addition
Closed under scalar multiplication

such that if a,b in F and u,v,w in V then

u+(v+w) = (u+v)+w
u+v = v+u
Additive identity exists 0 in V s.t. u+0 = u
Additive inverse exists a+ (-a) = 0

Multiplicative identity exist 1 in F s.t. 1*u = 1

a(bu) = (ab)u
(a+b)u = au+bu

a(u+v) = au + av

Subspace
Non-Empty Subset that is
Closed under addition
Closed under scalar multiplication

Has a basis/is a vector space

Disjoint Subspaces
Intersection is empty

Intersection of Subspaces
Set of vectors in both subspaces
Has a basis/is a vector space

Sum of subspaces
Set of all linear combinations of all vectors in both subspaces

Direct Sum
Sum of Vector spaces that are disjoint