Sudan University of Science and Technology

College of Science

Department of Mathematics

Rings And Linear Transformation's

A project Submitted in fulfillment for the degree of B.Sc. (Honor) in Mathematics

By :

1- Ayat Mohmmed Hassan
2- Somia Musa Idress
3- Heba Musa Idress

Supervisor:

Dr. Belgiss Abdelaziz

September 2015

Dedication

To our mothers and fathers

To our family and my tribe

To our teachers

To our colleagues and my colleagues

To our burn candles that illuminate for others

He taught me to each the characters

But above all to my prophet MOHAMED

Acknowledgment

First I would like to thank without end to our greater ALLAH, then I would like to express about my appreciation and thanks to our

Supervisor: Dr. BelgissAbdelaziz

and thanks for everyone help me...

Researchers...

Abstract

First we study some basic concept of ring and homomorphism of ring, we prove some theorem’s of ring’s and ideal and we give an example of subring.

Also we study the characteristic of ring.

Also we study the idempotent and nilpotent elements.

We study the vector space,field’s.

Final we study inner product space and nor of vector.

The Contains

subject	Page
الاستهلالية	I
Dedication	II
Acknowledgments	III
Abstract	IV
The Contains	V
Chapter 1 The Rings	1
Chapter 2 Vector Space	14
Chapter 3 Fields	51
Reference	59

Def (1.1):

Anon empty set R from a ring if the following axioms are satisfied:

(i) $a+(b+c)=(a+b)+c$ for all $a,b\in R$

(ii) $a+b=b+a$for all $a,b\in R$

(iii) $\exists$ some element 0 in R , s.t $a+0=0+a=a$for all $a\in R$

(iv) For each $a\in R$, $\exists$ an element $\left(-a\right)\in R, s.t\, a+(-a)=(-a)+a=0$

(v) $a.(b.c)=(a.b).c$for all $a,b,c\in R$

(vi) $a.(b+c)=a.b+a.c(b+c).a=b.a+c.a$for all $a,b,c\in R$

Remarks :

Since we say that $+\ and\ .$ are binary compositions on R under stood that the closure properties w.r.t these hold in R . in other words ,for all $a,b\in R$, $a+b\ and\ a.b$ are unique in R .

-In fact the statement that R in a ring would mean that R has two binary composition $+\ and\ .$ defined on it and satisfied the above axioms .

-The ring $(R,+)$ forms an abelian group .

Def (1.2):

A ring R is called a commutative ring if $ab=ba$ for all $a,b\in R.$

If $\exists$ an element $e\in R$ $s.tae=ea$ for all $a,b\in R$ it is also called unit element or multiplicative identity.

Remark:

We recall that in a group by a^2 we mean $a.a$ was binary composition of the group .

Theorem (1.3):

In a ring R the following results hold

(i) $a.0=0.a=0$ for all $a,b\in R$

(ii) $a(-b)=(a)b=-ab$for all $a,b\in R$

(iii) $(-a)(-b)=ab$

(iv) $a(b-c)=ab-a$

Proof:

(i) $a.0=a.(0+0)\Longrightarrow a.0=a.0+a.0\Longrightarrow a.0+0=a.0+a.0$

using cancelation w.r.t $+$ in the group $(R,+)$

(ii)$a.0=0\Longrightarrow a(-b+b)=0\Longrightarrow a(-b)+ab=0\Longrightarrow a(-b)=-(ab)$

similarly $(-a)b=-ab.$

(iii) $(-a)(-b)=-[a(b)]=-[-ab]=ab$

(iv) $a(b-c)=a(b+(-c)=ab+a(-c)=ab-ac$

Remark:

if n,m are integers and a,b elements of a ring then it is easy to see that

$n(a+b)=na+nb$

$(n+m)a=na+ma$

$(nm)a=n(ma)$

$a^m a^n=a^{mn}$

$(a^m)^n=a^{mn}$

We are so much used to the property that we every $ab = 0$ then either $a = 0 \; or \; b = 0$ but the convincing is not true ,"these property holds" in the ring of integers we have

$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq 0 B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \neq 0$ but $\quad AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$

Def (1.4):

Let R be a ring . An element $0 \neq a \in R$ is called a zero-divisor if there exist an element $a \neq b$ such that , $ab = 0 \; or \; ba = 0$.

Def (1.5):

A commutative ring R is called an integral domain if $ab = 0$ in ether $a = 0 \;\; or \; b = 0$, if a ring has no zero divisor .

Theorem (1.6):

A commutative ring R is an integral domain iff for all $a, b, c \in R \, , a \neq 0$

$$ab = ac \Rightarrow b = c$$

Proof:

Let R be an integral domain

$ab = ac \quad (a \neq 0) \quad then \quad ab - ac = 0 \quad \Rightarrow a(b - c) = 0$

$\Rightarrow a = 0 \;\; or \;\; b - c = 0 \quad since \quad a \neq 0 \;\; \Rightarrow b = c$

Conversely , let the given condition hold.

Let $a, b \in R$ be any elements with $a \neq 0$

suppose $ab = 0 \;\; , \; ab = a.0 \quad \Rightarrow b = 0$

hence $ab = 0 \;\; \Rightarrow \;\; b = 0$ whenever $a \neq 0$ or that R is integral domain .

Def (1.7):

A ring R is the said to satisfy left cancellation law if for all $a, b \in R$

$ab = ac \quad \Rightarrow \quad b = c \quad and \quad ba = ca \;\; \Rightarrow \quad b = c$

Def (1.8):

(1) A ring R an element a in a ring with unity called invertible (or a unity) w.r.t multiplication if there exist $b \in R$ such that $a.b = b.a =$**1**

(2) A ring R whose non zero element of R from a group under multiplication is a called a division ring, a commutative division ring is afield.

Now we get example to division ring which is not a field . let M be the set of all 2×2 matrices of the type $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ where a, b are complex number and $\bar{a}, \bar{b}$ are their conjugate. But M will not be a field as it is not commutative as

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

But

$$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

Theorem (1.9):

A field is an integral domain .

Proof :

Let $(R,+,.)$ be a field then R is commutative ring . now let $a.b=0$ in R we want to show that either $a=0\ or\ b=0$ suppose $a\neq 0$ then exists $a.b=0 \Longrightarrow a^{-1}(a.b)=a^{-1}0 \Longrightarrow b=0 \Longrightarrow R$ is an integral domain

Theorem (1.10):

A non zero finite integral domain is a field .

Proof :

Let R be a non zero finite integral domain , and let R' be the subset of containing non zero elements of R.

Since a associativity hold in R , it will hold in R' thus R' is a finite semi group Hence R' is a finite semi group w.r.t multiplication in which cancellation laws hold.

$\therefore (R',.)$ forms a group

In other words $(R,+,.)$ is a field (it being commutative as it is an integral domain).

Remark :

An infinite integral domain which is not a field is the ring of integers .

Problem(1) :

Show that a Boolean ring is commutative .

Solution:

Let for $a,b\in R$ be any elements then $a+b\in R$ by given condition

$$(a+b)^2=a+b$$
$$\Longrightarrow a^2+b^2+ab+ba=a+b$$
$$\Longrightarrow\ a+b+ab+ba=a+b$$
$$\Longrightarrow\ ab+ba=0 \qquad \longrightarrow (1)$$
$$\Longrightarrow\ ab=-ba$$
$$\Longrightarrow a(ab)=a\,(-ba)$$
$$\Longrightarrow a^2b=-aba$$
$$\Longrightarrow ab=-aba \qquad \longrightarrow (2)$$

From (1) and (2) we get

$$(ab)a=(ba)a$$
$$\Longrightarrow aba=-ba^2=-ba \quad \longrightarrow (3)$$

From (2) and (3) we get

$$ab=ba=-aba$$

$\Longrightarrow R\ is$ commutative ring .

Problem (2):

Show that an element a in z_n is a unity iff a and n are relatively prime.

Solution :

$z_n=[0,1,2,\dots,n-1]\ mod\ n$

Let $a\in z_n$be a unit,then there exist $b\in z_n\ \ s.t a\otimes b=1$

i.e when a b is divided by n , in other words

$$ab=nq+1\ \ or\ ab-nq=1$$

$\Rightarrow a\ and\ n$ are relatively prime

Now let $(a,n)=1$ then there exists integers u,v s.t $au+nv=1$ or $\Rightarrow au=n(-v)+1$

Suppose $u=nq+r\,,\quad 0\le r<n\,,\ r\in z_n$

i.e$a\otimes r=1 \qquad r\in z_n \Rightarrow a\ is\ unit$.

Problem (3):

If in a ring R , with unity $(xy)^2=x^2y^2$ for all $x,y\in R$ then show that R is commutative .

Solution :

Let $x,y\in R$ be any elements . then $y+1\in R$ as $1\in R$

By given condition

$$(x(y+1))^2=x^2(y+1)^2$$
$$\Rightarrow (xy+x)^2=x^2(y+1)^2$$
$$\Rightarrow (xy)^2+x^2+\frac{1}{2}yx+xxy=x^2(y^2+1+2y)$$
$$\Rightarrow x^2y^2+x^2+xyx+xxy=x^2y^2+x^2+2x^2y$$
$$\Rightarrow xyx=x^2y \qquad \longrightarrow (1)$$

Since (1) holds for all x,y in R we get

$$(x+1)y(x+1)=(x+1)^2y$$
$$\Rightarrow (xy+y)(x+1)=(x^2+1+2x)y$$
$$\Rightarrow x^2y+xy+yx+y=x^2y+y+2xy$$
$$\Rightarrow yx=xy \qquad using\ (1)$$

Hence R is commutative.

Problem (4):

Show that the ring R of real valued continues function on [0,1] has zero divisors .

Solution:

Consider the functions f and g defined on [0,1] by

$f(x)={}^1\!/_2-x \quad , \quad 0\le x\le {}^1\!/_2 \quad , \quad f(x)=0 \quad , \quad {}^1\!/_2\le x\le 1$

And

$g(x)=0 \quad , \quad 0\le x\le {}^1\!/_2 \quad , \quad g(x)=x-{}^1\!/_2 \quad , \quad {}^1\!/_2\le x\le 1$

Then f , g are continues functions and $f\ne 0 \quad , \quad g\ne 0$

$$\Rightarrow gf(x)=g(x)f(x)=0.\left({}^1\!/_2-x\right) \qquad if\ \ 0\le x\le {}^1\!/_2$$
$$=\left(x-{}^1\!/_2\right).0=0 \qquad if\ {}^1\!/_2\le x\le 1$$

i.e$gf(x)=0 \quad for\ all\ x$

$$\Rightarrow gf=0 \quad but \quad f\ne 0 \quad , \quad g\ne 0$$

Sub Ring

Def (1.11):

A non empty subset S of a ring R is a said be a subring of R if S form a ring under the binary compositions of R.

The ring $< z, +, . >$ of integers is a subring of the ring $< R, +, . >$ of real number.

if R is a ring then $\{0\}$ and R are always subring of R , called trivial subring of R.

Theorem (1.12):

A non empty subset S of a ring R is a subring of R iff$a, b \in S \Longrightarrow ab, a - b \in S$

Proof:

Let S be a subring of R then

$a, b \in S \Longrightarrow ab \in S\ (closure)$

$a, b \in S \Longrightarrow a - b \in S$

as $\langle S, +\rangle$ is a subgroup of $\langle R, +\rangle$

conversely, since $a, b \in S \Longrightarrow a - bS$,we fined $\langle S, +\rangle$ forms a subgroup of $\langle R, +\rangle$ A gain for any $a, b \in S$ since $S \subseteq R$

$a, b \in R \Longrightarrow a + b = b + a$

And so we a fined S is abelian.

In other words ,S satisfies all the axioms in the definition of a ring Hence S is a subring of R.

Sum of Two sub Rings

Def (1.13):

Let S and T be two subring of a ring R .we define

$$S + T = \{s + t | s \in S\,, t \in T\}$$

Def(1.14):

let R be a ring ,the set $Z(R) = \{x \in R | xr = rx,\ for\ all\ \ r \in R\}$ is called centre of the ring .

problem(1) :

if R is a division ring then show that the centre $Z(R)$ of R is a field .

Solution:

$Z(R)$ is a ring (as it is a subring)

$Z(R)$ is commutative by its definitions.

$Z(R)$ has unity as $1. x = x. 1 = x$ for all $x \in R$.

Thus we need show that every non zero element of $Z(R)$ has multiplicative inverse (in $Z(R)$).

Let $x \in Z(R)$ be any non zero element .

Then $x \in R$ and since R is a division ring ,$x^{-1} \in R$.

Let $y \in R$ be any non zero element ,then $y^{-1} \in R$. Now

$$x^{-1}y = (y^{-1}x)^{-1} = (xy^{-1})^{-1} = yx^{-1}$$

$\Longrightarrow x^{-1}$commutes with all non zero elements of R

Again as $\quad x^{-1}.0 = 0.x^{-1} = 0$

We fined $\quad x^{-1}r = r.x^{-1} \quad for\, all\, r \in R \Longrightarrow x^{-1} \in Z(R)$

Showing $Z(R) is\ a\ field$

Problem(2) :

If in a ring R the equation $ax = b$ for all $a, b \ (a \neq b)$ has a solution, show that R is a division ring .

Solution :

We first show that are has no zero division , suppose

$$ab = 0\,, a \neq 0, b \neq 0$$

As $a \neq 0\ , ax = a$ has a solution ,say $x = e_1$then $ae_1 = a$

Again $bx = e_1$ has a solution , let $x = e_2$ be a solution of this $be_2 = e_1$

Now $\quad ab = 0 \Longrightarrow (ab)e_2 = 0.e_2 = 0$

$$\Longrightarrow a(be_2) = 0 \Longrightarrow ae_1 = 0$$

$$\Longrightarrow a = 0\ \ , but\ \ a \neq 0$$

Hence R without zero divisor

Now for any $a \neq 0 ax = a$ has solution, let $x = e$ be solution then $ae = a \Longrightarrow aex = ax \quad for\ all\ x \quad \Longrightarrow a(ex - x) = 0 \ \ for\ all\ x$ or that e is left identity .

Again $(xe - x)e = xee - xe = x(ee) - xe = xe - xe = 0$ (as e is left identity) ,but $e \neq 0, thus\ xe - x = 0\ \ or\ xe = x\ \ \ for\ all\ x$

i.e e is right identity .

now equation $ax = e$ has a solution for all $a \neq 0 \Longrightarrow \exists b\ \ s.t\ \ ab = e$

hence a has right invers . since right identity also exists , $\langle R, . \rangle$ Forms a group or the R is a division ring .

Remark:

In continuation to the above problem we make the following observations.

(a) $\langle Z, +, . \rangle$ Has same unity 1 as that of its parent ring $\langle E, +, . \rangle$.

(b) Finally, we notice we can have a ring without unity which has a subring with unity. Take for instance, the ring

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | a, b \in Z \right\}$$

Now if $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ is unity of this ring then $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & a \\ 0 & 0 \end{bmatrix}$ should be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ i.e $a = 1$

Also $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ should be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ i.e $a = 1 = b$

Therefor if R has unity then it must be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ but

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} . \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ hence R has no unity

It is easy to check that $S=\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} |a\in Z\right\}$ is a subring of R and has unity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Characteristic of a Ring

Def(1.15):

Let R be a ring . if there exists a positive integer n such that $na=0$ for all $a\in R$ then R is said to have finite characteristic and also the smallest such positive integer is called the characteristic of R

If no such positive integer exists then R is said to have characteristic zero (or infinity).

If ch of a ring is n then ch of any subring or extension ring is also n.

Theorem (1.16):

Let R be a ring with unite . if **1** is of additive order n then $ch\,R=n$. If 1 additive order infinity then $ch\,R$ is 0.

Proof:

Let additive order of 1 be n .then $n.1=0$ and n is such last +iv integer now for any $x\in R$.

$$nx=x+x+\cdots+x=1.x+1.x+\cdots+1.x$$
$$=(1+1+\cdots+1)x=0.x=0$$

Showing $ch\,R=n$.

Has infinite order under addition then ∃ no n s.t $n.1=0$ and thus .

Remark :

(i) The above result can be stated as. If R is a ring with unity then R has $ch\,n>0$ iff n is the smallest positive integer s.t $n.1=0$

(ii) Ch of Z_n ring of integers modulo n is n.

Problem :

If D is an integral domain then characteristic of D is ether zero or a prime number .

Proof :

If $ch\,D$ is the zero , we have nothing to proof . suppose D has finite characteristic then ∃ a +ve integer m s.t $ma=0$ for all $a\in D$

Let k be least +ve integer then $ch\,D=k0$,we show k is a prime .Suppose k is not a prime , then we can write

$$k=rs \quad ,1<r \quad ,s<k$$

Now

$$ka=0 \qquad for\ all\ a\in D$$
$$\Longrightarrow (rs)a^2=0 \quad \forall a\in D$$
$$\Longrightarrow a^2+a^2+\cdots+a^2=0 \ \ (rs\ times\ )$$
$$\Longrightarrow (a+a+\cdots+a)(a+a+\cdots+a)=0$$
$$\Longrightarrow (ra)(sa)=0 \quad \forall a\in D$$

$$\Rightarrow ra = 0 \;\; or \;\; sa = 0 \qquad \forall a \in D \; (D \; is \; integral \; domain)$$

In either case it will be a contradiction as $r, s < k$ but k is the ieast +ve integer s.t $ka = 0$.

problem :

If D is an integral domain and if $na = 0$. For sum $0 \neq a \in D$ and some integer $n \neq 0$ then show that the characteristic of D is finite .

Solution :

Since $na = 0$

$$(na)x = 0 \;\; for \; all \; x \in D$$
$$\Rightarrow (a + a + \cdots + a)x = 0$$
$$\Rightarrow ax + ax + \cdots + ax = 0 \; (n \; times)$$
$$\Rightarrow a(x + x + \cdots + x) = 0 \;\; for \; all \; x \in D$$
$$\Rightarrow x + x + \cdots + x = 0 \; for \; all \; x \in D \quad as \; a \neq 0$$
$$\Rightarrow nx = 0 \; for \; all \; x \in D \;\; , n \neq 0$$
$$\Rightarrow ch \; D \; is \; finite$$

Def (1.17):

An element e in a ring R is called idempotent if $e^2 = e$. An element $a \in R$ is called nilpotent if $e^n = 0$ for some positive integer n .

If R is a ring with unity ,then 0 and 1 are idempotent element. Also 0 is nilpotent element of R.

Problem:

a non zero idempotent cannot be nilpotent .

Solution:

let x be non zero idempotent , then $x^2 = x$ if x is also nilpotent then $\exists$ integer $n \geq 1 \;\; s.t x^n = 0$ But

$$x^2 = 0 \Rightarrow x^3 = x^2 = x$$
$$\Rightarrow x^4 = x^2 = x$$

$\Rightarrow \; x^n = x \Rightarrow x = 0$ a contradiction.

Problem:

In an integral domain R (with unity) the only idempotent are the zero and unite .

Solution :

Let $x \in R$ be any idempotent then

$$x^2 = x \Rightarrow x^2 - x = 0 \Rightarrow x(x - 1) = 0 \Rightarrow x = 0 \;\; or \; x = 1$$

As R is an integral domain .

Product of Ring

Let R_1 and R_2be two ring. Let $R = \{(a, b) | a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1,b_1).(a_2,b_2)=(a_1a_2,b_1b_2)$$

problem :

if R and S are two ring , then

$ch\ (R\times s)=0$ if $ch\ R=0$ or $ch\ S=0$

$=k$ where $k=l.c.m(ch\ R, ch\ S)$

Solution :

Let $ch\ R=0$ and suppose $ch\ (R\times S)=t\neq 0$ then

$$t(a,b)=(0,0)\ \forall a\in R\ ,b\in S$$

$\Longrightarrow (ta,tb)=(0,0)\Longrightarrow ta=0\ \ \forall a\in R,$ a contradiction as $ch\ R=0$ thus $ch\ (R\times S)=0$

Similarly, if $ch\ S=0$,then $ch\ (R\times S)=0.$

Let now $ch\ R=m\ \ ,ch\ S=n\ \ and\ let\ K=l.c.m.(m,n)$

Then $k(a,b)=(ka,kb)=(0,0)\ \ \forall a\in R\ \ ,\ \ b\in S$ as m,n divide k

Suppose $p(a,b)=(0,0), then\ (pa,pb)=(0,0)$

$$\Longrightarrow pa=0=pb\Longrightarrow m|p\ ,n|p$$
$$\Longrightarrow k|b\Longrightarrow k\leq p\Longrightarrow ch\ (R\times S)=k$$

Def(1.18):

A non empty subset I of a ring R is a called a right ideal of R if

(i) $a,b\in I\Longrightarrow a-b\in I$

(ii) $a\in I,\ \ \Longrightarrow r\in R\Longrightarrow ar\in I$

I is a called a left ideal R if

(i) $a,b\in I\Longrightarrow a-b\in I$

(ii) $a\in I,\ \ \Longrightarrow r\in R\Longrightarrow ra\in I$

For example let $\langle Z,+,.\rangle$ Be the ring of integers . then $E=set$ of even integers in an ideal of Z $a,b\in E\Longrightarrow a=2n\ \ ,\ \ b=2n$ thus

$$a-b=2(n-m)\in E$$

Again , if $2n\in E\ \ ,r\in Z$ then as $(2n)r\ or\ \ r(2n)$ are both in E ,E is an ideal .

Problem :

Let S be a non empty subset of a ring R . show that

$r(s)=\{x\in R|Sx=0\}$ and $l(s)=\{x\in R|Sx=0\}$ are respectively right and left ideal of R.

Solution :

$r(s)\neq\varphi\ as\ \ 0\in r(s)$, again $x,y\in r(s)\Longrightarrow sx=0\ \ ,sy=0$ now

$$S(x-y)=Sx-Sy=0-0=0\Longrightarrow x-y\in r(s)$$

Again if $r\in R$ by any element then

$$S(xr)=(sx)r=0.r=0\Longrightarrow xr\in r(s)$$

Hence $r(s)$ is a right ideal. Similarly , $l(s)$ will form a left ideal .

$r(s)$ and $l(s)$ are called right and left annihilators of S, respectively .

$r(s)$ and $l(s)$ would both be ideal of R if S is an ideal .(verifty!)

problem :

let R be a ring such that every subring of R is an ideal of R. further $ab = 0\ in\ R \Longrightarrow a = 0\ \ or\ b = 0$. show that R is commutative.

Solution :

Let $0 \neq a \in R$ be any element .

Then $N(a) = \{x \in R|xa = ax$ is a subring of R and therefore an ideal of R . let $r \in R$ be any element Since $a \in N(a)\,, r \in R$ we find $ra \in N(a)$(def. of ideal) also then $a(ra) = (ra)a$ and so

$$(ar - ra)a = 0 \Longrightarrow ar - ra = 0\ \ as\ a \neq 0$$

Thus $ar = ra\ \ \ \forall\, r \in R\ \ ,\ \ \forall\, 0 \neq a \in R$ and as $0.s = r.0 = 0$ we find

$$Ar = ra \qquad \forall a, r \in R$$

Hence R is commutative.

Sum of Two Ideal

Let A and B be two ideals of a ring R . we define $A + B$ to be the set $\{a + b|a \in A\,, b \in B\}$ called sum of the ideal A and B .

Theorem (1.19):

if A and B are two ideals of R then A+B is an ideal of R , containing both A and B.

proof :

$A + B \neq \varphi\ \ as\, 0 + 0 \in A + B$ Again $x, y \in A + B \Longrightarrow x = a_1 + b_1$
$y = a_2 + b_2\ \ \ for\ some\ \ \ \ a_1, a_2 \in A\,,\ \ b_1, b_2 \in B$ since

$$x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

we find $\ \ x - y \in A + B$

let $x = a + b \in A + B\,, r \in R$ be any element then

$xr = (a + b)r = ar + br \in A + B$ as A, B are ideals

$$rs = r(a + b) = ra + ba \in A + B$$

Thus A+B is an ideal of R.

Again for any $a \in R$, since $a = a + 0 \in A + B$ and for any $b \in B$, since $b = 0 + b \in A + B$. we fined $A \subseteq A + B\ \ \ ,\ \ \ B \subseteq A + B$.

Remark :

we can show that A is an ideal of A+B.

$a_1, a_2 \in a \Longrightarrow a_1 - a_2 \in A$ as A is an ideal of R .again if $a \in A\ and\ s \in A + B$ be any element then $s = a_1 + b_1$ for some $a_1 \in A\,, b_1 \in B$ also

$$as = a(a_1 + b_1)$$

$$= aa_1 + ab_1 \in A \text{ as } a, a_1 \in A \ \Longrightarrow aa_1 \in A$$

$$a \in A\,, b_1 \in B \subseteq R \Longrightarrow ab_1 \in A \Longrightarrow aa_1 + ab_1 \in A$$

Similarly $sa \in A$ showing that A is an ideal of A+B

Def(1.20):

Let S be subset of a ring R .An ideal A of R is the said to be generated by S if

(i) S$\subseteq A$

(ii) For any ideal I of R ,$S \subseteq I\ \ \Longrightarrow A \subseteq I$

We denote it by writing $A = \langle S\rangle\ or\ A = (s)$

In fact $< S >$ will be intersection of all ideals of R that contain S ,and is the smallest ideal containing S. if S is finite, we say $A =< S >$ is finite generated .

Theorem (1.21):

if a and B two ideal of R, then $A + B =< A \cup B >$.

Proof :

We have already proved that A+B is an ideal of R ,containing A and B thus A+B is an ideal containing $A \cup B$.

Let I be any ideal of R s.t $A \cup B \subseteq I$

Let $x \in A + B$ be any element then $x = a + b$ for some $a \in A \quad , \quad b \in B$ since

$$a \in A \subseteq A \cup B \subseteq I$$
$$b \in B \subseteq A \cup B \subseteq I$$

We fined $a + b \in I$ as I is an ideal

$$\Longrightarrow x \in I \;\; or\, that\, A + B \subseteq I$$

Example :

Let (E,+,.) be the ring of even integers. It is commutative ring without unity. let $a = 4 \in E$. Then

$$< 4 > = \{4n + (2m)4|n, m \in Z\}$$
$$= \{4n + 8m|n, m \in Z\}$$

Whereas $4E = \{4(2k)|k \in Z\} = \{8k|k \in Z\}$

We notice then $< 4 >\neq 4E$ as $4 \in< 4 > \;\; but \;\; 4 \notin 4E$.

Problem :

If A is an ideal of a ring R with unity such that $I \in A$ then show that $A = R$.

Solution :

Since $A \subseteq R$ always ,all we need show is that $R \subseteq A$. Let $r \in R$ be any element .

Since $I \in A$ and A is an ideal $\quad r = 1.r \in A \Longrightarrow R \subseteq A$ or that A=R.

Problem :

Show by means of any example that we can fined $A \subseteq B \subseteq R$ where A is an ideal of B ,B is an ideal of R ,but a is not an ideal of R.

Solution :

Let R be the set containing matrices of the type $\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{bmatrix}$ over integers then R forms a ring under matrix addition and multiplication . Take

$$A = \left\{ \begin{bmatrix} 0 & 0 & x \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} |x\; an\; integer \right\}$$

$$B = \left\{ \begin{bmatrix} 0 & 0 & u \\ 0 & 0 & v \\ 0 & 0 & 0 \end{bmatrix} |u, v\ integers \right\}$$

It would be easy to verify that A is an ideal of B, B is an ideal of R. to see that A is not an ideal of r, we notice

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \notin A$$

Product of Two Ideal

Let A,B be two ideal of a ring R. we defined the product AB of A and B by $AB = \{\sum a_i b_i | a_i \in A\ , b_i \in B\}$

Where summation is finite

Theorem(1.22):

The product AB of any two ideals A&B of a ring R is an ideal of R.

Proof :

Let ,y ∈ AB $\neq \varphi$ as $0 = 0.0 \in AB$

Then $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

$$y = a'_1 b'_1 + \cdots + a'_m b'_m$$

For some $a_i , a'_i \in A , b_i\ , b'_j \in B$

$$x - y = (a_1 b_1 + a_2 b_2 + \cdots + a_n b_n) - (a'_1 b'_1 + \cdots + a'_m b'_m)$$

Which clearly belongs to A,B as the R.H.S can written as

$$x_1 y_1 + x_2 y_2 + x_k y_k (k = n + m)$$

Where $x_i \in A$, $y_i \in B$

Again for any $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in AB\ \ and\ r \in R$

$$rx = r(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)$$

$$= (ra_1) b_1 + (ra_2) b_2 + \cdots + (ra_n) b_n \in AB$$

Because $ra_i \in A\ \ as\ a_i \in A$, $r \in R$, and A is an ideal

Similarly $xy \in AB$

Showing there by that AB is an ideal of R.

problem :

if A as a left and B is a right ideal of a ring R then show that AB is a two sided ideal of R whereas AB need not be even a one – sided ideal of R.

Solution :

That AB will be a two sided ideal of R follows by the theorem above. We show by an example that BA need not be even a one-sided ideal

Take $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} |a, b \in Z \right\}$

$$B = \left\{ \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} |c, d \in Z \right\}$$

In the ring R of 2x2 matrices over integers then as seen earlier A is left and B is a right ideal of R.

BA would have members of the type $\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$

i.e. of the type $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, x ∈**Z**

Now if we type $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in BA and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ in R

Then $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin BA$

$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin BA$

Hence BA is nether a left nor a right ideal of R.

The motivating factor in rings was set -of integers and in groups the set of all permutations of a set. A vector space originates from the notion of a **vector** that we are familiar with in mechanics or geometry. Our aim in this volume is not to go into details of that. Reader would recall that a vector is defined as - a directed line segment, which in algebraic, terms is defined as an ordered pair (a, *h)* , being coordinates of the terminal point relative to a fixed coordinate system. Addition of vectors is given by the rule-$(a_1, b) + (a_2, b_2) = (a_1 + \boldsymbol{a_1}, b_1 + b_2)$One can easily verify that set' of vectors• under this forms an a belian group.

Also scalar multiplication is defined by the rule a $(a, b) = (aa, a\beta)$ which satisfies certain properties.This concept is extended similarly to three dimensionS. We generalise the whole idea through definition of a vector space and vary the scalarsnot only in the set of real's but in any field *F.* A vector space thus differs from groups and rings in as much as it also involves elements from outside itself.

Def(2.1):

Let <*V,* + >be an abelian group and <*F,* +.>be a field. Define a function (called scalar multiplication) from $F \times V \longrightarrow V$,s.t., for all $a \in F, v \in V$, $a\,.\boldsymbol{v} \in V$. Then *V* is said to form a *vector space* **over** *F* if for all $x, y \in \boldsymbol{V}$, $a\beta \in F$, the following hold

(i) $(a + \beta)x = ax + \beta x$

(ii) $a(x + y) = ax + ay$

(iii) $(a\beta)x = a(\beta x)$

(iv) $1\,.x = x$,1 being unity of *F.*

Also then, numbers of *F* are called *scalars* and those of *V* are called vector S.

Remark:

We have used the same symbol + for the two different binary compositions of *V* and *F,* for convenience.Similarly same symbol **.** is used for scalar multiplication and product of the field *F.*

Since <*V,* + >is a group, its identity element is denoted by 0. Similarly the field F would also have zero element which will also be represented by 0. in case of doubt one can use different symbols like 0_v and 0_F etc.. Since we generally Workwith afixed field we hal1 only ho writing V isa space (or Sometimes *V (F)* or V_F) I would always be understood that it is a vector space over *F* (unless stated otherwise) .

We defined the scalar multiplication from $F \times V \longrightarrow V$. One can also define it from $F \times V \longrightarrow V$ and have a similar definition. The first one is .called a left vector space and the second a right vector space. it is easy to show that if *V* is a left vector space over *F* then it is a right vector space over *F* and conversely. In view this result it becomes redundant to talk about left or right vector spaces. We shall thus talk of only vector spaces over *F*.

One can also talk about the above system when the scalars are allowed to take values in a ring instead of a field, which leads us to the definition of modules

Theorem (2.2):

In any vector space V(F) the following results hold

(i) $0.x = 0$

(ii) $a.0 = 0$

(iii) $(-a)x = -(ax) = a(-x)$

(iv) $(a - \beta)x = ax - \beta x$

Proof:

$0.x = (0+0).x = 0.x + 0.x \Rightarrow 0 + 0.x = 0.x + 0.x \Rightarrow 0 = 0.xx$ (cancellation in *V)*

(i) $a.0 = a(0+0) = a.0 + a.0 \Rightarrow a.0 = \mathbf{0}$

(ii) $(-a).x + ax = [(-a) + a]x = 0.x = 0$

(iii) follows from above

Example :

If <*F,* + **,** . >be a field, then F is a vector space $< F, + > = < V, + >$is an additive abelian group. Scalar multiplication can be La as the product of *F.* All properties are seen to hold . Thus *F(F)* is a vector space ***S***.

Example:

Let *P* = set of all polynomials over a field *F,* then *P* forms a vector space under addition and scalar multiplication defined by

$$f(x) + g(x) = (f+g)x$$
$$a(fx)) = (af)\,(x)\;a\;aF$$

Subspaces:

Def(2.3):

A non empty subset W of a vector space V(F) is said to form a subspace of V if W forms a vector space under the operations of V.

Theorem (2 ,4):

necessary and sufficient condition for a non empty subset W of a vector space V(F) to be a subspace is that W is closed under addition and scalar multiplication.

Proof:

If W is a subspace , the result follows by definition.

Conversely, let W be closed under addition and scalar multiplication.

$$Let\ x, y\ \in\ W, since\ I \in F\ \ , -1\ \in F$$
$$-1, y \in W \Rightarrow y \in W$$
$$x, -y \in W = x - y \in W$$

$\Rightarrow < W, + >$forms a subgroup of $<V, + >$

Rest of the conditions in the definition follows trivially.

Theorem (2.5):

A non empty subset W of a vector space V(F) is a subspace of V iff $ax + \beta y \in W\ for\ a, \beta \in F\ ,\ x, y \in W.$

Proof :

If W is a subspace, result follows by definition.

Conversely, let giver condition hold in W.

$Let\ x, y \in W$ be any elements. Since $1 \in\ F$

$$1. x + 1. y = x + y \in W$$

$\Rightarrow W$ is closed under addition.

Again,$\boldsymbol{x} \in\ W, a \in F$ then

$$ax =\ ax\ + 0. y\quad for\ any\ y \in W,\ \ 0 \in F$$

which W. (Note here 0 may not be in W)

Hence W is closed under scalar multiplication. The result thus follows by previous theorem.

Problem:

Show that union of two subspaces may not be a subspace

Solution:

$W_1 \cup W_2$will be the set containing all pairs of the type $(a, 0)$, $(0, b)$In particular $(1, 0), (0, 1) \in W_1 \cup W_2$ But , $(1,0) + (0, 1)\ (1, 1)\ \notin W_1 \cup W_2$. Hence $W_1 \cup W_2$is not a subspace. Reader is referred to exercises for more results pertaining to intersection, union of subspaces.

Sum of Subspaces

If $W_1 and\ W_2$be two subspaces of a vector space *V(F)* then, we define

$$W_1 + W_2 = \{w_1 + w_2 | w_1 \in W_1\ ,\qquad w_2 \in W_2\}$$
$$W_1 + W_2 \neq \varphi\ \ as\ 0 = 0 + 0 \in W_1 + W_2$$

Again,$x, y \in W_1 + W_2\ \ \ ,\ \ a, \beta \in \boldsymbol{F}$implies

$$x = w_1 + w_2$$
$$\boldsymbol{y} = w'_1 + w'_2 w_1, w'_1 \in W_1\ \ ,\ \ \ w_2, w'_2 \in W_2$$
$$ax + \beta y\ =\ a\ (w_1 + w_2) + \beta(w'_1 + w'_2)$$

$$= \left(aw_1 + \beta w'_1\right) + (aw_2 + \beta w'_2) \in W_1 + W_2$$
Showing thereby that sum of two subspaces is a subspace.

Def(2.6):
We say a vector space V is the *direct sum* of two subspace $W_1$and W_2if

(i) $V = W_1 + W_2$

(ii)every $v \in \boldsymbol{V}$ can be expressed uniquely as the sum $w_1 + w_2 \in \boldsymbol{F}$and $w_2 \in W_2$
and in that case we write $V = W_1 \oplus W_2$

Theorem(2.7):
$$V = W_1 \oplus W_2 \Leftrightarrow V = W_1 + W_2\,, W_1 \cap W_2 = (0)$$
Proof:
Let $V = W_1 \oplus W_2$
We need prove $W_1 \cap W_2 = (0)$
Let
$$x \in W_1 \Longrightarrow x \in W_1 \; and \; x \in W_2$$
$$\Longrightarrow x = 0 + x \in W_1 + W_2 = V$$
$$\Longrightarrow x = x + 0 \in W_1 + W_2 = V$$
Since x has been expressed as $x = x + 0$ and $0 + x$ and the representation has to be unique, we get $x = 0 \Longrightarrow W_1 \cap W_2 = (0)$
Conversely, let $v \in V$ be any element an suppose
$$v = w_1 + w_2$$
$$v = w'_1 + w'_2$$
are two representations of v then ,
$$w_1 + w_2 = w'_1 + w'_2 (= v) \;\; \Longrightarrow w_1 - w'_1 = w'_2 - w_2 = 0$$
Now L.H.S. is in$W_1$and RH.S belongs , to W_2, i.e each belongs to
$$W_1 \cap W_2 = (0)$$
$$\Longrightarrow w_1 - w'_1 = w'_2 - w_2 = 0$$
$$\Longrightarrow w_1 = w'_1\,, w_2 = w'_2$$
Hence the result.

Example :
Consider the space $V(F) = F^2(F)$ where F is a field.

solution :
Let $W_1 = \{(a,0)|a \in F\} \quad , \qquad W_2 = \{(0,b)|b \in F\}$
then V is direct sum of W_1 and W_2
$$v \in V \Longrightarrow v = (a,b) = (a,0) + (0,b) \in W_1 + W_2$$
thus $V \subseteq W_1 + W_2 \quad , \; or \; that \;\; V = W_1 + W_2$
Again if $(x,y) \in W_1 \cap W_2$ be any element then
$$(x,y) \in W_1 \; and \; (x,y) \in W_2 \Longrightarrow y = 0 \;\; and \;\; x = 0 \Longrightarrow (x,y) = (0,0)$$
$$\Longrightarrow W_1 \cap W_2 = (0)$$

Hence $V = W_1 \oplus W_2$

Problem :

Let V be the vector space of all functions from $\boldsymbol{R} \longrightarrow \boldsymbol{R}$ Let $V_e = \{f \in V | f is\ even\} V_0 = \{f \in V | f is\ odd\}$.Then$V_e$and V_0 are subspaces of V and $= V_e \oplus W_2$.

Solution :

Addition and scalar multiplication in V are given by the rule

$$(f+g)x = f(x) + g(x)\ ;\ (af)x = af(x)$$

Now$V_e \neq \varphi\ \ as\ 0(-x) = 0(—x) = 0 \Longrightarrow 0(x) = 0(-x) \Longrightarrow 0 \in V_e$

Again for $a, \beta \in R$, $f, g \in V_e$ we have

$$(af + \beta g)(-x) = (af)(-x) + (\beta g)(-x) = a(f(-x) + \beta\big(g(-x)\big)$$

$$= af(x) + \beta g(x) = (af + \beta g)x$$

$$\Longrightarrow af + \beta g \in V_e$$

⟹V is a subspace of V

Similarly ,$V_e + V_0$ is a subspace of V.

Thus $V_e + V0$ is a ubspace of V. We show $V \subseteq V_e + V_0$ .Let $f \in V$ be any member ,Let g : $\boldsymbol{R} \longrightarrow \boldsymbol{R}$ e such that $g(x) = f(-x)$, then $g \in V$, Also then

$$f = \left(\frac{1}{2}f + \frac{1}{2}g\right) + (\frac{1}{2}f - \frac{1}{2}g)$$

Since

$$\left(\frac{1}{2}f + \frac{1}{2}g\right)(-x) = \frac{1}{2}f(-x) + \frac{1}{2}g(-x) = \frac{1}{2}g(x) + \frac{1}{2}f(x)$$

$$= \left(\frac{1}{2}f + \frac{1}{2}g\right)x$$

We fined $\frac{1}{2}f + \frac{1}{2}g \in V_e$

Similarly , $\frac{1}{2}f - \frac{1}{2}g \in V_0 \Longrightarrow f \in V_e + V_0 \Longrightarrow V \subseteq V_e + V_0$ or that $V = V_e + V_0$

Finally $f \in V_e \cap V_0 \Longrightarrow f \in V_e , f \in V_0$

$$f(-x) = f(x) and\ f(-x) = -f(x)$$

$$\Longrightarrow f(x) = -f(x) \Longrightarrow f(x) + f(x) = 0 = 0(x)$$

$$\Longrightarrow 2f(x) = O\ (x)\ for\ all\ x$$

$$\Longrightarrow 2f = O \Longrightarrow f = \ \ V_e \cap V_0 = (0)$$

Hence the result .

Problem :

If L, M ,N are three subspaces of a vector space V, such that $M \subseteq L$then show that

$$L \cap (M + N) = (L \cap M) + (L \cap N) = M + (L \cap N).$$

Also give an example, where the result fails to hold when M ⊈ L .

Solution :

We Jeave the first part for the reader to try. Recall a similar result was proved for ideals in rings. The equality is- called modular equality.

Consider now the vector space $V = R^2$

Let

$$L = \{(a, a)|a \in R\}$$
$$M = \{(a, 0)|a \in R\}$$
$$N = \{(0, b)|b \in R\}$$

It is a routine matter to cheek that L, M, N are subspaces of V. indeed

$$a(a, a) + a(a, . a)(, a', a') = (aa, aa) + (\beta a', \beta a')$$
$$(aa + \beta a', aa + \beta a') \in L\ etc$$

$Now\ (x, y) \in L \cap M \Rightarrow (x, y) \in L\ and\ (x, y) \in \mathrm{M} \Rightarrow y = x\ and\ y = 0$

$$x = O = y \Rightarrow (x, y) = (0,0)$$

Similarly, $L \cap N = \{(0, 0)\}$

$$L \cap N = \{(0, 0)\}$$

Again,

$$M + N = \{(a, b)|a, b \in R\} and\ as(1,1) \in M + N \ \ , (1, 1) \in L$$

we find $(1, 1) \in L \cap (M + N), but\ (1, 1) \notin L \cap M + L \cap N$

Hence $L \cap (M + N \neq (L \cap M) + (L \cap N), when\ M \nsubseteq L$

Quotient Spaces

If W be a subspace of a vector space V(F) then since <W, +> forms an abelian group of < V,+ >,we can talk of cosets of W in V. Let be the set of all cosets$W + v, v \in V$, then we show that$\frac{V}{W}$ also forms a vector space over F, under the operations defined by

$$(W + x) + (W + y) = W + (x + y) \quad x, y€V$$
$$a(W + x) = W + ax \quad a \in F$$

Addition is well defined, since,

$$W + x = W + x'$$
$$w + y = W + y'$$
$$\Rightarrow x - x' \in W \ \ , \ \ y - y' \in W$$
$$\Rightarrow (x - x') + (y - y') \in W$$
$$\Rightarrow (x + y) - (x' + y') \in W$$
$$\Rightarrow W + (x + y) = W + (x' + y')$$

Again $W + x = W + x'$

$$\Rightarrow x - x' \in W$$
$$\Rightarrow a(x - x) \in W \ \ , a \in F$$
$$\Rightarrow ax - ax' \in W$$
$$\Rightarrow W + ax = W + ax'$$
$$\Rightarrow a(W + x) = a(W + x')$$

$W + 0$ will be zero of$\frac{V}{W}W - x$ will be inverse of $W + x$ Also

$$a\left((W + x) + (W + y)\right) = a\left(W + (x + y)\right) = W + a(x + y)$$

$$\begin{aligned} &= W + (ax + ay) \\ &= (W + ax) + (W + ay) \\ &= a(W + x) + a(W + y)\ etc. \end{aligned}$$

Hence, V/W forms a vector space over F, called the quotient space of V by W.

Homomorphism Or Linear Transformations

We are already familiar with the concept of a homomorphism in case group and rings. We introduce the same in vector spaces.

Def(2.8):

Let V and U be two vector spaces over the same field F, then a mapping $T: V \longrightarrow U$ is called a homomorphism or a linear transformation if

$$T(x + y)T(x) + T(y)\ for\ all\ \ x, y \in V$$

$$T(ax) = aT(x) \quad\ a \in F$$

One can combine the two conditions to get a single condition

$$T(ax + \beta y) = aT(x) + \beta T(y) \quad x, y \in V\ ,\ a, \beta \in F$$

It is easy to see that both are equivalent. If a homomorphism happens to be one - one onto also we call it an isomorphism, and say the two spays are isomorphic.

(Notation $V \cong U$)

Example :

(i) Identity map $: V \longrightarrow V$ s.t $I(v) = v$

and the zero map $O: V \longrightarrow V$ s.t $O(v) = 0$ are clearly linear transformations.

(ii) For a field F, consider the vector spaces F^2 and. Define, a map $: F^3 \longrightarrow F^2\ , by\ T(a, \beta, \gamma) = (a, \beta)$.

then T is a linear transformation as

for any $x, y \in F^3, if\ x = (a_1, \beta_1, \gamma_1)\quad ,\quad y = (a_2, \beta_2, \gamma_2)$ then

$$\begin{aligned} T(x + y) = T(a_1 + a_2, \beta_1 + \beta_2, \gamma_1 + \gamma_2) &= (a_1 + a_2, \beta_1, \beta_2) \\ &= (a_1, \beta_1) + (a_1, \beta_2) = T(x) + T(y) \end{aligned}$$

And

$$\begin{aligned} T(ax) = T\big(a\ (a_1, \beta_1, \gamma_1)\big) &= T(aa_1, a\beta_1, a\gamma_1) = (aa_1, a\beta_1) \\ &= a(a_1, \beta_1) = aT(x) \end{aligned}$$

(i) Let V be the vector space of all polynomial□ in x over a field F. Define

$$T: V \longrightarrow N\ , s.t.$$

$$T\big(f(x)\big) = \frac{d}{dx}\, f(x)$$

then $T(f + g) = \frac{d}{dx}(f + g) = \frac{d}{dx}\, f + \frac{d}{dx}\, g = T(f) + T(g)$

$$T(af) = \frac{d}{dx}(af) = a\frac{d}{dx}\, f = aT(f)$$

show that T is linear transformation. In fact, if $U: V \longrightarrow V$ be defined such that $\int_0^x f(t)dt$,then U will also be a linear transformation.

In the theorems that follow, we take V and U to be vector spaces

Theorem(2.9):

Under a homomorphism $T: V \longrightarrow U$

(i) $T(0) = 0$

(ii) $T(-x) = -T(x)$.

Proof :

$T(0) = T(0 + 0) = T(0) + T(0)$ ⇒T(0) =0

Again

$$T(-x) + T(x) = T(-x + x) = T(0) = -T(x) = T(-x).$$

Def(2.10):

Let $T: V \longrightarrow U$ be a homomorphism, then kernel of T is a subspace of F.

Proof:

$Ker\ T \neq \varphi\ as$ $0 \in \ker T$ by any elements then

$$T(ax + \beta y) = aT(x) + \beta T(y) = a.0 + \beta.0 = 0 + 0 = 0$$

$$\Longrightarrow ax + \beta y \in \ker T$$

Theorem(2.11) :

Let $T: V \longrightarrow U$ be a homomorphism, then

$Ker\ T = \{O\}$ iff T is one-one.

Proof :

Let $Ker\ T = \{O\}$. If $T(x) = T(y)$

then $T(x) - fly) = 0$

$$\Longrightarrow T(x - y) = 0$$

$$\Longrightarrow (x - y) \in Ker\ T = \{0\}$$

$$\Longrightarrow x = y$$

Conversely, let T be one - one

if $x \in Ker\ T$ be any element, then $T(x) = 0$

$$\Longrightarrow T(x) = T(0)$$

$$\Longrightarrow x = O$$

$$\Longrightarrow Ker\ T = \{0\}.$$

Def(2.12):

Let $T: V \longrightarrow U$ be a linear transformation then range of T is defined to be.

$$T(V) = \{T(x) | x \in V = Range\ T = R_T = \{u \in U | u = T(v), v \in V\}$$

Theorem(2.13):

Let $T: V \longrightarrow U$ be a LT. (linear transformation) then range of T is a subspace of U.

Proof :

Since $T(0) = 0$, $0 \in V$, $T(0) \in Range\ T$ i.e. $Range\ T \neq \varphi$

Let $a, \beta \in F, T(x), T(x) \in T(V)$ be any elements then $x, y \in V$ Now $aT(x) + \beta T(y) = T(ax + \beta y) \in T(V)$ as $ax + \beta y \in V$

Hence the result.

Note : T(V) = U iff T is onto.

Theorem(2.14):

Let $T: V \longrightarrow U$ be a L.T. then

$$\frac{V}{\ker T} \cong Range\ T = T(V)$$

Proof :

Let $T: V \longrightarrow U$ and put $Ker\ T = K$, then K being a subspace of V, we can talk of V/K.

Define a mapping $\theta: V/K \longrightarrow T(V)$, s.t $\theta(K+x) = T(x)\ , x \in V$

Then θ is will defined one-one map as

$$\begin{aligned} K + x \ &= \ K + y \\ \Leftrightarrow x - y &\in K = Ker\ T \\ \Leftrightarrow T(x-y) &= 0 \\ \Leftrightarrow T(x) &= T(y) \\ \Leftrightarrow \theta(K+x) &= \theta(K+y) \end{aligned}$$

If $T(x) \in T(V)$be any element, then $x \in V$ and $\theta(K+x) = T(x)$, showing that θ is onto .

Finally

$$\begin{aligned} \theta\big((K+x)+(K+y)\big) &= \theta\big(K+(x+y)\big) \\ &= T(x+y) = \ T(x) + \ T(y) \\ &= (K+x) + \theta(K+y) \end{aligned}$$

$$\theta(a\big((K+x)\big) = \theta(K+ax) = T(ax) = aT(x) = a\theta(K+x)$$

shows θ is L.T. and hence an isomorphism. .

Note :

The above is called the Fundamental Theorem of homomorphism vector spaces.

If the map T is also onto, then we have proved $\frac{V}{\ker T} \cong \ U$.

Theorem(2.15):

If A and B be two subspaces of a vector space V(F)

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

Proof :

A being a subspace of $A+B$ and $A \cap B$ being a subspace of B, we can talk of $\frac{A+B}{A}$ and $\frac{B}{A \cap B}$

Define a map $\theta: B \longrightarrow \frac{A+B}{A}$ st. $\theta(b) = A + b\ , b \in B$

Since $b_1 = b_2$, we find θ is well defined.

Again as $\theta(b_1 + b_2) = \ A + (ab_1 + \beta b_2)$

$$\begin{aligned} &= (A + ab_1) + (A \ + \beta b_2) \\ &= a(A + b_1) + \beta(A + b_2) \\ &= a\theta(\theta) + \beta\theta(b_1) \end{aligned}$$

θ is a L.T

For any $+x \in \frac{A+B}{A}$, we find $x \in A+B$

$$x = a+b, \; a \in A\,, b \in B$$

$$A + x = A + (a+b)$$

$$(A+a) + (A+b) = A + (A+b) = A+b = \theta(h)$$

Showing that 1, is the required pre image of $A + x$ under O and thus O is onto. Hence by Fundamental theorem

$$\frac{A+B}{A} \cong \frac{B}{\ker\theta}$$

We claim $Ker\ \theta = A \cap B$

Indeed

$$x \in \ker\theta \Leftrightarrow \theta(x) = A \Leftrightarrow A + x = A$$

$$\Leftrightarrow x \in A, \qquad also\ \ x \in Ker\ \theta \subseteq B \Leftrightarrow x \in A \cap B$$

Hence

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

Note :

By interchanging A and B, we get. $\frac{B+A}{B} \cong \frac{A}{B \cap A}$ i.e $\frac{A+B}{A} \cong \frac{B}{A \cap B}$

Corllory : If A+B is the direct sum then as $A \cap B = \{0\}$ we get

$$\frac{A}{(0)} \cong \frac{A \oplus B}{B}$$

But $\frac{A}{(0)} \cong A$ gives us $A \cong \frac{A \oplus B}{B}$.

Theorem (2.16):

Let W be a subspace of V then an onto L.T. $\theta : V \longrightarrow \frac{V}{W}$ such that $Ker\ \theta = W$ '

Proof :

Define $\theta : V \longrightarrow \frac{V}{W}$ s.t $\theta(x) = W + x$.

then θ is clearly well defined .Also

$$\theta(ax + \beta y) = W + (ax + \beta y)$$

$$= (W + ax) + (W + \beta y)$$

$$= a(W + x) + \beta(W + y) = a\theta(x) + \beta\theta(y)$$

Shows θ is a L.T.

$\theta$is dourly onto.

Again $x \in Ker\ \theta \Leftrightarrow \theta(x) = W \Leftrightarrow W + x = W \Leftrightarrow x \in W$

Hence $Ker\ \theta = W$.

T is called the natural homomorphism or the quotient map.

Remark :

In case W=(0) in the above we find θ will be $1-1$ also as

$$\theta(a) = \theta(b) \Longrightarrow W + a = W + b$$

$$\Rightarrow\ a-b\in W=(0)$$
$$\Rightarrow a-b=0$$
$$\Rightarrow\ a\ =b.$$

Hence in that case $V\cong\frac{V}{W}\ or\ V\cong\frac{V}{(0)}$

Note $W\ =(0)=Ker\ \theta\ =(0)=\theta$ is one - one.

Problem :

Let W and U be subspaces of V(F) such that $W\subset U\subset V$ let $V\colon V\longrightarrow\frac{V}{W}$ be the quotient map. Show that $\theta\colon V\longrightarrow\frac{V}{W}f(U)$ is a proper subspace of $\frac{V}{W}$

Solution :

Since f is a L.T., f(U) is a subspace of V/W.

$If\ f(U)=0$ then $f(x)=0$ for all $x\in U$

$$\Rightarrow W+x=\ W\ forall\ \ x\in U$$
$$\Rightarrow x\in W\ \ forall\ \ x\in U$$

$\Rightarrow U\subseteq W,$ a contradiction

Again since $U\neq V,\exists\ v_0\in V\ s.t\quad v_0\notin U$

If $f(\ v_0)\in f(U)$ then $f(\ v_0)=f(x)$ for some $x\in U$

$$\Rightarrow f(\ v_0-x)=\ 0$$
$$\Rightarrow W+\ (\ v_0-x)=W$$
$$\Rightarrow\ v_0-x\in W$$
$$\Rightarrow x\ +w\ \ for\ some\ \ w\in W$$

$\Rightarrow 0\in U$, a contradiction of hence $f(\ v_0)\in f(U)\Rightarrow\ f(U)\neq\frac{V}{W}$ or that $f(U)$is proper subspace of V/W.

Theorem (2.17):

Let $V\ \longrightarrow U$ be an onto homomorphism with $Ker\ T=W$ then there exists a one-one onto mapping between the subspaces of U and the subspace of V which contain W

Proof :

Let **A** =set of all subspaces of V, which contain W

R =set of all subspaces of U

Define a mapping θ:**A** $\longrightarrow$ R s.t

$$\theta(W_1)\ =\ T(W_1)$$

Since $T\colon V\longrightarrow\ U$, $T(W_1)$ will be a subspace of U as for any $T(x),T(y)\ \in\ T(W_1)$ and $a,\beta\in F$

$$aT(x)+T(y)\in T(ax+\beta y)\in T(W_1),as\ x,y\in W_1$$

Again $W_1=W_1'\Rightarrow T(W_1)\ =\ T(W_1{}')\Rightarrow\theta$ is well define

Now if $\theta(W_1)=\theta(W_1{}')$.

Then $T(W_1)\,T(W_1{}')\Rightarrow W_1=W_1{}'$

As $x\in W_1\ \Rightarrow\ T(x)\in T(W_1)=\ T(W_1')$

$$\Rightarrow\ T(x)\in T(W_1')\Rightarrow\ T(x)=T(y),\qquad y\in W_1$$
$$\Rightarrow T(x-y)=0$$

$$\Rightarrow x - y \in Ker\, T \;=\; W_1 \subseteq W_1'$$
$$\Rightarrow W_1 \in W_1' \; as \;\; y \in \; W_1{}'$$

$W_1 \subseteq W_1'$Similarly $W_1{}' \subseteq W_1$

Hence θ is 1—1.

Let U_1 e be any member.

Define $T(U_1) \;=\; \{x \in V | T(x) \in U_1)$

Then $0 \in T^{-1}(U_1)\, as \;\; T(O) = 0 \in U_1 For\, a, \beta \in F \;\; , \;\; x, y \in T^{-1}(U_1)$, we have $T(x) \in U_1 \;, \; T(y) \in U_1$

$$aT(x) + \beta T(y) \in U_1 \Rightarrow T(ax + \beta y) \in U_1 \Rightarrow ax + \beta y \in T^{-1}(U_1)$$

Or that $T^{-1}(U_1)$ is subspace of V.

Let $x \in \; Ker\, T \Rightarrow T(x) = 0 \in U_1$

$$\Rightarrow x \in T^{-1}(U_1) \Rightarrow W \subseteq T^{-1}(U_1)$$
$$\Rightarrow T^{-1}(U_1) \in A$$

also

$$T\left(T^{-1}(U_1)\right) = \{T(x) \in V | T(x) \in U_1\} \subseteq U_1$$

let

$y \in U_1 \;\; \Rightarrow y \in U \Rightarrow \exists\, x \in V\; s.t\, T(x) = y$

as T is onto $x \in T^{-1}(U_1) \Rightarrow y \;=\; T(x) \in T^{-1}(U_1))$

$$\Rightarrow T\big(T^{-1}(U_1)\big) = U_1$$
$$\theta\big(T^{-1}(U_1)\big) = U_1$$
$$\Rightarrow \;\; \theta \; is \; onto$$

Hence the theorem is proved.

Liner Span

Def(2.18) :

Let V(F) be a vector space, $v_i \in V$, $a_i \in F$ be elements of V and F respectively .Then element of the type $\sum_{i=1}^{n} a_i v_i$ are called linear othina of $v_1, v_2, \ldots v_n$over F.

Let S be a non empty subset of V, then the set

$$L(S) = \left\{ \sum_{i=1}^{n} a_i v_i \,| v_i \in V \;, \qquad a_i \in F\;, v_i \in S\;, \qquad a_i \in F \;\;, n\, finite \right\}$$

i.e the set of ail linear combinations of finite sets of elements of S is called linear span of S. It is also denoted by <S>.

Theorem (2.19):

L(S) is the smallest subspace of V, containing S.

Proof :

$$L(S) \neq \varphi \; as \;\; v \in S \Rightarrow v = 1.v \;, 1 \in F \Rightarrow v \in L(S).$$

thus, in fact, $S \subseteq L(S)$.

Let $x, y \in L(S), \quad a, \beta \in F$ be any elements then

$$x = \; a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$
$$y = \beta_1 v'_1 + \beta_2 v'_2 + \cdots + \beta_m v'_m$$

Thus

$$ax \ +\beta y = aa_1v_1 + aa_2v_2 + \cdots + aa_nv_n + \beta\beta_1v'_1 + \beta\beta_2v'_2 + \cdots + \beta\beta_mv'_m$$

R.H.S. being a liner combination belongsto L(S) .Hence $L(S)$ is a subspace .V containing S.

Let now W be any subspace of V containing S

We show $L(S) \subseteq W$

$$x \in L(S) \Rightarrow x = \sum a_iv_i \quad , \qquad a_i \in F \,, v_i \in S$$

$v_i \in S \subseteq W$ for all i and W is a subspace

$$\Rightarrow \sum a_iv_i \in W \Rightarrow x \in W \Rightarrow L(s) \subseteq W$$

Hence the result follows.

Theorem(2.20):

If $S_1$and$S_2$are subsets of V then

(i) $S_1 \subseteq S_2 \Rightarrow L(S_1) \subseteq L(S_2)$

(ii) $L(S_1 \cup S_2)\ L(S_1)\ +\ L(S_2)$

(iii) $L(L(S_1)) =\ L(S_1)$

Proof :

(i) $x \in L(S_1) \Rightarrow\ x = \sum a_iv_i\ v_i \in S_1\ ,\ a_i \in F$thus $v_i \in S_1 \subseteq S_2$ for all i

$$\Rightarrow \sum a_iv_i \in S_1 \Rightarrow x \in L(S_2)$$

$$\Rightarrow L(S_1) \subseteq L(S_2)$$

(ii) $S_1 \subseteq S_1 \cup S_2 \Rightarrow L(S_1) \subseteq L(S_1 \cup S_2)$

$$S_2 \subseteq S_1 \cup S_2 \Rightarrow L(S_2) \subseteq L(S_1 \cup S_2)$$

$$\Rightarrow L(S_1) + L(S_2) \subseteq L(S_1 \cup S_2)$$

Again $S_1 \subseteq L(S_1) \subseteq\ L(S_1) + L(S_2)$

$$S_2 \subseteq L(S_2) \subseteq L(S_1)\ + L(S_2)$$

hence $S_1 \cup S_2 \subseteq L(S_1) + L(S_1)$

$$L(S_1 \cup S_2) \subseteq L(S_1) + L(S_1)$$

as $L(S_1 \cup S_2)$ is the smallest subspace containing $S_1 \cup S_2$and $L(S_1) +\ L(S_2)$ is a subspace, being sum of two subspaces (and contains $S_1 \cup S_2$).

Thus $\quad L(S_1 \cup S_2) = L(S_1)\ + L(S_2)$

(iii) Let $L(S_1) =\ K$ then we show $L(K) = L(S_1)$

Now $K \subseteq L(K)$

$\therefore\ L(S_1) \subseteq L(L(S_1))$

Again $x \in L(L(S_1))\ x$ is linear combination of members of L(S_1) which are linear combinations of members of S_1.

So x is a linear combination of members of $S_1 \Rightarrow x \in L(S_1)$

Thus $\quad L(L(S_1))\ \subseteq L(S_1)$ hence $L\big(L(S_1)\big) = L(S_1)$.

Theorem (2.21) :

If W is a subspace of V then L(W) and conversely.

Proof :

$W \subseteq L(\ W)$ by definition and since L(W) is the smallest subspace of containing W and W is itself a subspace

$$L(W) \subseteq W$$

Hence $L(\mathrm{W}) = \mathrm{W}$

conversely let $L(W) = W$, let $x, y \in W$, $a, \beta \in F$ then $x, y \in L(W)$

$\Rightarrow$ x, y are liner combination of members of W.

$\Rightarrow$ $ax + \beta y$is liner combination of members of W.

$$\Rightarrow ax + \beta y \in L(W)$$

$$\Rightarrow ax + \beta y \in W$$

$\Rightarrow$W is a subspace.

Def(2.22):

If V = L(S), we say S spans (or generates) V. The vector space V is said to be finite - dimensional (dyer F) if there exists a finite subset S of V. such that V = L(S) . We use notation F.D. V.S. for a finite dimensional vector space.

It now follows, from the results we proved that ,1f S_1 and S_2. are two subspaces of V, then $S_1 + \ S_2$ is the subspace spanned by $S_1 \cup S_2$

Indeed, $L(S_1 \cup S_2) = L(S_1) + L(S_2) = S_1 + S_2$

Problem:

Let $S = \{(1,4), (0,3)\}$ be a subset of $\boldsymbol{R}^2(\boldsymbol{R})$ Show that (2.3) belongs to L(S).

Solution:

$(2, 3) \in L(S)$ if it can be put as a linear combination of (1,4) and (0, 3)

Now

$(2, 3) = a(1, 4) + \beta(0, 3) \Rightarrow (2,3) = (a + 0\ , 4a + 3\beta)$

$$\Rightarrow 2\ =\ a\ , 4a\ + 3\beta = 3\beta \Rightarrow a\ = 2\ \ , \beta - \frac{5}{3}$$

hence $(2,3) = 2\ (1,4) - \frac{5}{3}\ (0,3)$ Showing that $(2,3) \in L(s)$

Linear Dependence and Independence

let V(F) be a vector space. elements $v_1, v_2, ... v_n$ in V are said to be linearly dependent (over F) if ∃ scalars $a_1, a_2, ..., a_n \in F$. (not all zero) such that

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$$

($v_1, v_2, ... v_n$are finite in number, not essentially distinct).

Thus for linear dependence $\sum a_iv_i = 0$. and at least one $a_i \neq 0$. If $v_1, v_2, ... v_n$are not linearly d'pendent (L.D.) these are called linearly independent(L.I).

In other words,$v_1, v_2, ... v_n$are L.I. if

$$\sum a_i v_i = 0 \quad , a_i = 0 \ for\ all\ i$$

A finite set $X = \{x_1, x_2, \dots, x_n\}$ is said to be L.D. or L.I. according as its n members are L.D. or L.I.

In general any subset Y of V(F) is called L.I , if every finite non empty subset of Y is L.I , otherwise it is called L.D.

So, if some subsets are L.I. and some are L.D. then Y is called L.D.

Observations:

(i) A non zero vector is always L.I. as $v \neq 0$, $av = 0$ would mean $a = 0$.

(ii) Zero vector is always L.D. , $1.0 = 0 \quad 1 \neq 0$, $1 \in F$.

Thus any collection of vectors to which zero belongs is always L.D

In other words, if $v_1, v_2, \dots v_n$are L.I then none of these can be zero. (But not conversely, see example ahead).

(i) V is L.I iff$v \neq 0$

(ii) Empty set φ is L.I. since it has no non empty finite subset and consequently it satisfies the condition for linear independence. In other words, whenever $\sum a_i v_i = 0$ in φ then as there. is no i for which $a_i \neq 0$, set is L.I. We sometimes express it by saying that empty set is L.I. vacuously.

Examples:

(i) Consider $\boldsymbol{R}^2(\boldsymbol{R}), \boldsymbol{R}$ = reals.

$$v = (1,0)\ , \qquad v_2 = (0,1) \in \boldsymbol{R}^2 \ are\ L.I$$

as $\quad a_1 v_1 + a_2 v_2 = 0 \quad for \quad a_1, a_2 \in \boldsymbol{R}$

$$\Rightarrow a_1(1,0) + a_2(0,1) = (0,0)$$

$$\Rightarrow (a_1, a_2) = (0,0) \Rightarrow a_1 = a_2 = 0.$$

(ii) Consider the subset $S = \{(1,0,0), (0,1,0), (0,0,1), (2,3,4)\}$ in the vector space $\boldsymbol{R}^3$ (R).

Since $2(1,0,0) + 3(0,1,0) + 4(0,0,1) - 1(2,3,4) = (0,0,0)$ we find S is L.D .

In the vector space P of polynomials the vectors $(x) = 1 - x$, $g(x) = x - x^2$, $h(x) = 1 - x^2$are L.D. since $f(x) + g(x) - h(x) = 0$. .

Problem :

Show that the vectors

$$v_1 = (1,1,2,4) \quad , \quad v_2 = (2,-1,-5,2) \quad ,$$

$$v_3 = (1,-1,-4,0) \quad and \quad v_4 = (2,1,1,6)$$

are L.D in $\boldsymbol{R}^4$ (R).

Solution :

Suppose $av_1 + bv_2 + cv_3 + dv_4 = 0$, $\quad a, b, c, d \in R$ then

$$a(1,1,2,4) + b(2,-1,-5,2) + c(1,-1,-4,0) + d(2,1,1,6) = (0,0,0,0)$$

$$\Rightarrow a + 2b + c + 2d = 0$$

$$a - b - c + d = 0$$

$$2a - 5b - 4c + d \ = \ 0$$

$$4a + 2b + 0c + 6d = 0$$

$$\Rightarrow \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & -1 & -1 & 1 \\ 2 & -5 & -4 & 1 \\ 4 & 2 & 0 & 6 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$R_1 \to R_2 - R_1, R_3 \to R_3 - 2R_1, R_4 \to R_4 - 4R_1$$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$R_4 \to R_2 - R_1 \ , R_3 \to \frac{1}{3} R_3$$

$$\begin{bmatrix} 1 & 2 & -1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -1 & -\frac{2}{3} & -\frac{1}{3} \\ 0 & -\frac{3}{4} & -1 & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$R_4 \to R_4 - R_2 \ , R_3 \to R_3 - R_2$$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow a + 2b + c + 2d \ = \ 0$$

$$-3b - 2c - d = \ 0$$

$$3b + 2c + \ +d = 0$$

$a \ = 1 \ , \ b = 1 \ , \ c = 1 \ , \ d = 1$ satisfy the equations. .

Since coefficients are non zero, the given vectors are L.D.

Problem:

If two vectors are L.D. then one of them is the scalar multiple of the other

Solution :

Suppose $v_1, v_2$are L.D. then $\exists a_i \in F$s.t

$$a_1 v_1 + a_2 v_2 = 0 \quad for\ some\ a_i = 0$$

Without loss of generality we can take $a_1 \neq 0$then ${a_1}^{-1}$ exists and $a_1 v_1 = (-a_2 v_2) \Rightarrow v_1 = (-{a_1}^{-1} a_2) v_2 = \beta v_2$

which proves the result.

Problem:

If x, y, z are L.I. over the field C of complex nos. then so are $x + y \ , \ y + z \ \ and \ \ z + x$ over C.

Solution :

Suppose $a_1(x+y)+a_2(y+z)+a_3(z\ +x)=\ 0\ ,\ \ a_i\in C$

Then $(a_1+a_3)x+(a_1+a_2)y\ +(a_2+a_3)z=0$

$$\Rightarrow a_1+a_3=a_1+a_2=a_2+a_3=0\quad ,\qquad as\ \ x,y,z\ \ are\ L.I.$$

Solving we find.

$$a_1=a_2=a_3=0$$

Hence the result.

Note :

Linear dependence depends not only upon the vector space , but the field as well.

Consider, for instance, **C(C), C(R), C** = complex, **k**= real's .

Take $1\ ,\ i\in C\ \ ,if\quad a,\beta\in R$.then $a.1+\beta.i\ =0=0\ +i0$

$\Rightarrow a=0\quad ,\ \beta=0\quad \Rightarrow$1, I are L.I. in **C(R)**

Now if we take a,β In C , then as we can take $a=1$ ‘ $\beta=\ -1$, so that

$$i.1+(-1)i=0\ we\ fined\ \exists\ a,\beta\neq 0$$

s.t sums of the type $\sum a_iv_i=0$

i.e1 , i are L.D iv **C(C).**

Def(2.23):

Let V(F) be a vector space. A subset S of V is called a basis of V if S consists of L.I. elements (i.e., any finite number of elements in S are L.I.) and $V=L(S)$, i.e S spans V.

Theorem(2.24):

let $S\ =\{v_1,v_2,\dots v_n\}$ is a basis of V, then every element of V can be expressed uniquely as a linear combination of $v_1,v_2,\dots v_n$

Proof:

Since, by definition of basis, $V=L(S)$ each element $v\in V$ can be expressed as n linear combination of $v_1,v_2,\dots v_n$ Suppose

$$v=a_1v_1{+}a_2v_2+\cdots+a_nv_na_i\in F$$
$$v=\beta_1v_1+\beta_2v_2+\cdots+\beta_nv_n\beta_i\in F$$

Then $a_1v_1{+}a_2v_2+\cdots+a_nv_n=\beta_1v_1+\beta_2v_2+\cdots+\beta_nv_n$

$$\Rightarrow(a_1-\beta_1)v_1+(a_2-\beta_2)v_2+\cdots+(a_n-\beta_n)v_n=0$$

$\Rightarrow a_i\beta_i=0$ for all I $(v_1,v_2,\dots v_n\ are\ L.I)$

$$\Rightarrow a_i=\beta_i\ \ for\ all\ i$$

Theorem(2.25):

Suppose S is a finite subset of a vector space V such that $V=L(S)$ [i.e., V is a F.D.V.S] then there exists a subset of S which is a basis of V .

Proof :

If S consists of L.I. elements then S itself forms basis of V and we’ve nothing to prove.

Let now T be a subset of S, such that T spans Vof S (Existence of T is ensured as S is finite)

Suppose $T = \{v_1, v_2, \dots v_n\}$

we show T is L.I.

Suppose $a_i \neq 0$for some i Without any loss of generality we can take$a_1 \neq 0$Then ${a_1}^{-1}$ exists.

$$a_1v_1{+}a_2v_2 + \cdots + a_nv_n = 0$$
$$\Rightarrow {a_1}^{-1}(a_1v_1{+}a_2v_2 + \cdots + a_nv_n) = 0$$
$$\Rightarrow v = (-{a_1}^{-1}a_2)v_2 + (-{a_1}^{-1}a_3)v_3 + \cdots + (-{a_1}^{-1}a_n)v_n$$
$$= \beta_2v_2 + \beta_3v_3 + \cdots + \beta_nv_n\beta_i \in F$$

If $v \in V$ be any element then

$$v = \gamma_1v_1{+}\gamma_2v_2 + \cdots + \gamma_nv_n\gamma_i \in F \quad as\ V = L(T)$$
$$\Rightarrow v = \gamma_1(\beta_2v_2 + \cdots + \beta_nv_n) + \gamma_2v_2 + \cdots + \gamma_nv_n$$

i.e any element of V is a linear combination of $v_1, v_2, \dots v_n$.

$\Rightarrow v_1, v_2, \dots v_n$ spans V, which contradicts our choice of T (as T was such minimal)

Hence $a_1 = 0$ or that $a_i = 0$ for all $i \Rightarrow v_1, v_2, \dots v_n\ \ are\ L.I$

And thus t is a basis of F.

Def(2.26):

A F.D.V.S V is said to have dimension n if n is the number of elements in any basis of V .we use the notation dim_F V=n or simply dim V and say V is n−dimensional vector space .

In view of an example done earlier dim R^2=2

In fact , dim R^n=n .

Theorem(2.27) :

A F.D.V.S V has dimension n iff n is the maximum number of L.I. .vectors in any subset of V

Proof:

Let dim $V = n$ and let $\{v_1,v_2,\dots\dots v_n\}$ be a basis of V , then these are L.I..

Let S= $\{w_1,w_2,\dots\dots w_m\}$ *be* a subset of V where m $> n$. we show S must be L.D. set .

Since w_1 , w_2 , ………….w_m all belong to V and $\{v_1,v_2,\dots\dots v_n\}$ is a basis of V; we can write

$w_1 = a_{11}v_1 + a_{21}v_2 + \dots\dots + a_{n1}v_n$

$w_2 = a_{12}v_1 + a_{22}v_2 + \dots\dots + a_{n2}v_n a_{ij} \in$ F

…………

$w_m = a_{1m}v_1 + a_{2m}v_2 + \dots\dots + a_{nm}v_n$

Consider the following system of n equations in m unknowns

$a_{11}x_1 + \dots\dots + a_{1m}x_m = 0$

$$a_{n1}x_1 + \cdots \dots + a_{nm}x_m = 0$$

Since n <m , the above system has a non−zero solution α_1, ……$\alpha_m \in$ F (i.e., some $\alpha_i \neq 0$).

$$a_{11}\alpha_1 \ + \cdots \ldots + a_{1m}\alpha_m \ = \ 0$$

$$\ldots \ldots \ldots \ldots \ldots$$

$$a_{n1}\alpha_1 \ + \cdots \ldots + a_{nm}\alpha_m \ = \ 0$$

$$\Rightarrow a_{11}\alpha_1 v_1 \ + \cdots \ldots + a_{1m}\alpha_m v_1 \ = \ 0$$

$$\ldots \ldots \ldots \ldots \ldots$$

$$a_{n1}\alpha_1 v_n \ + \cdots \ldots + a_{nm}\alpha_m v_n \ = \ 0$$

$$\Rightarrow \alpha_1(a_{11}v_1 + \cdots \ + a_{n1}v_n) + \cdots .. + \alpha_m(a_{1m}v_1 + \cdots . + a_{nm}v_n) = \ 0$$

$\Rightarrow \alpha_1 w_1$ + ….. +$\alpha_m w_m$ = 0, where some $\alpha_i \neq 0$
$\Rightarrow w_1, w_2$,…………, w_m are L.D.
Which proves our result .

Conversely , let the maximum number of L.I. elements in any subset of V be n the there exists a subset , S =$\{v_1 , v_2 , \ldots \ldots v_n\}$ of V such that S is L.I. we claim S forms a basis of V.

Let v ∈ V be any element.

Let T = $\{v_1 , v_2 , \ldots , v_n, v\}$ than as it contains n+1 elements , it is L.D. ⇒ $\exists \alpha_1\alpha_2, \ldots, \alpha_n$, α in F such that

$\alpha_1 v_1 \ + \ \ldots \ldots + \alpha_n v_n \ + \ \alpha v \ = \ 0$ with some coefficients not zero.

Suppose α =0 then $\alpha_1 v_1 \ + \cdots + \alpha_n v_n$ = 0

⇒ α_i = 0 for all i as v_1,$v_2, \ldots, v_n$ are L.I.

i.e. all α_i and α are zero , which is not true . Hence $\alpha \neq 0 \Rightarrow \alpha^{-1}$ exists in F . now $\alpha \, v \ = -\alpha_1 v_1 \ - \ \alpha_2 v_2 \ - \ \ldots . -\alpha_n v_n$

$$\Rightarrow v \ = (-\alpha^{-1}\alpha_1)v_1 \ + \ (-\alpha^{-1}\alpha_2) \, v_2 \ + \cdots . + (-\alpha^{-1}\alpha_n) \, v_n$$

Or that v is linear combination of v_1 ,v_2 ……,v_n and v being any element , we find S spans V or that S forms basis of V.

Hence dim V = n.

Theorem(2.28) :

If V is a F.D.V.S. and $\{v_1, v_2, \ldots, v_r\}$ is a L.I. subset of V , then it can be extended to form a basis of V.

Proof :

If $\{v_1, v_2, \ldots, v_r\}$ spans V, then it itself forms a basis of V and there is nothing to prove

Let $S \ = \{v_1, v_2, \ldots, v_r, v_{r+1}, \ldots . , v_n\}$ be maximal L.I. subset of V. we show S is a basis of V , for which it is enough to prove that S spans V. Let v∈ V be any element .

Then T= $\{v_1, v_2, \ldots, v_n, v\}$ is L.D. by choice of S

⇒ $\exists \alpha_1, \alpha_2, \ldots . , \alpha_n$, α ∈ F(not all zero) such that

$\alpha_1 v_1 \ + \cdots + \alpha_n v_n$ +αv = 0

We claim $\alpha \neq 0$. Suppose α = 0

Then $\alpha_1 v_1 + \cdots \ldots + \alpha_n v_n$ = 0

⇒ α_i = 0 for all i as $v_1, v_2, \ldots, v_n$ are L.I.

∴ α= α_i = 0 for all i which is not true

Hence $\alpha \neq 0$ and so α^{-1} exists .
Since = $(-\alpha^{-1}\alpha_1)v_1$ + $(-\alpha^{-1}\alpha_2)v_2$+………+ $(-\alpha^{-1}\alpha_n)v_n$ v is a linear combination of v_1, v_2,……….v_n.
Which proves our assertion .

Theorem(2.29):

if dim $V = n$ and s {v_1, v_2,……….v_n.} spans V then S is a basis of V.

Proof :

since dim V=n , any basis of V has n elements . By theorem 17, a subset of S will be a basis of V but as S contains n elements , it will itself form basis of V .

Theorem(2.30):

if dim V = n and S= {v_1, v_2,……….v_n.}is L.I. subset of V then S is a basis of V.

Proof:

since {v_1, v_2,……….v_n.} =S is L.I. it can be extended to form a basis of V , but dim V being n , it will itself be a basis of V .

Problem:

If {v_1, v_2,……….v_n.} is a basis of F.D.V.S. V of dim n and v = $\sum \alpha_i v_i$ $\alpha_n \neq 0$ then prove that {v_1, v_2,……….v_{r-1}, v,v_{r+1},….v_n} is also a basis of V .

Solution :

we have
V = $\alpha_1 v_1$+…..+$\alpha_r v_r$ +…..+$\alpha_n v_n \alpha_r \neq 0$ ∴ ${\alpha_r}^{-1}$ exists
⇒ v_r= $(-\alpha^{-1}\alpha_1)v_1$ +…..+$(-{\alpha_r}^{-1}\alpha_{r-1})v_{r-1}$ +${\alpha_r}^{-1}$v+…. + $(-{\alpha_r}^{-1}\alpha_n)\alpha_n$

$$= \beta_1 v_1 + \cdots + \beta_{r-1}v_{r-1} + \beta_r v + \beta_{r+1}v_{r+1} + \cdots + \beta_n v_n$$

If x∈ V be any element, then

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \alpha_i \in F$$

⇒ $x = \alpha_1 v_1 + \cdots + \alpha_{r-1}v_{r-1} + \alpha_r(\beta_1 v_1 + \cdots + \beta_n v_n) + \cdots + \alpha v_n$ or that is a linear combination of

$$v_1, \dots, v_{r-1}, v, v_{r+1}, \dots, v_n$$

And x being any element , we find V is panned by $\{v_1, \dots, v_{r-1}, v, v_{r-1}, \dots, v_n\}$ and it forms a basis of V , using theorem done above .

Theorem(2.31):

Two finite dimensional vector spaces over F are isomorphic iffthey same dimension .

Proof :

Let V and W be two isomorphic vector spaces over F and let θ : $V \longrightarrow W$ be the isomorphism .
Let dim V =n and $\{v_1, v_2, \dots, v_n\}$ be a basis of V .

We claim { θ (v_1), (v_2) ,….., $\theta(v_n)\}$ is a basis of W.
Let $\sum_{i=1}^{n} \alpha\, \theta(v_1) = 0 \alpha_i \in$ F ,

$$\Rightarrow \qquad \sum \theta(\alpha_i v_i) = 0 = \theta(0)$$

$$\Rightarrow \qquad \sum \alpha_i v_i = 0 = (\theta\ is\ 1-1)$$

$$\Longrightarrow \alpha_i = 0 \quad for\ all\ \ i \quad as \quad v_1\,, v_2, \dots \dots ., v_n\ are \quad L.I.$$

$$\Longrightarrow \qquad \theta(v_1)\,, \theta(v_2), \dots \dots .., \theta(v_n)\ \ are\ L.I$$

Again, if $w\in W$ is any element, then as θ is onto,∃ some $v \in V$ s.t θ (v) = w

Now $\quad v \in V \Longrightarrow v = \sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$

$$\Longrightarrow w = \theta\,(v) = \theta\,(\sum \alpha_i v_i)$$

$$\Longrightarrow \quad w = \sum \theta(\alpha_i v_i) = \alpha_1 \theta(v_1) + \alpha_2 \theta(v_2) + \dots .. + \alpha_n \theta(v_n)$$

or that wis a linear combination of $\theta(v_1), \theta(v_2)\,, \dots \dots, \theta(v_n)$ Hence $\theta(v_1), \theta(v_2)\,, \dots \dots, \theta(v_n)$span W and therefore, form a basis *of* W showing that dim $W = n$. .
Conversely, let $dim\, V = \dim W = n$and suppose $\{v_1, v_2, \dots .. v_n\}$ and $\{w_1, w_2, \dots .. w_n\}$are basis of V and W respectively .
Define a map $O: V \to W$s.t.

$$\theta\,(v) = \theta\,(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_3 v_3)$$
$$= \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_n w_n$$

then θ is easily seen to be well defined (Indeed any $v \in V$ is a linear combination of members of basis) .
If v, $\acute{v} \in V$ be any elements then

$$v = \sum \alpha_i v_i, \acute{v} = \sum \beta_i v_i\, \alpha_i, \beta_i \in F$$

$$\theta(v + v') = \theta\left(\sum \alpha_i v_i + \sum \beta_i v_i\right)$$

$$= \theta(\sum(\alpha_i + \beta_i)v_i$$

$$= \sum(\alpha_i + \beta_i)w_i$$

$$= \sum \alpha_i w_i + \sum \beta_i w_i$$

$$= \theta(v) + \theta(v')$$

Also

$$\theta\ (\alpha v) = \theta\left(\alpha \sum \alpha_i v_i\right) = \theta\left(\sum \alpha\alpha_i v_i\right) = \sum(\alpha\alpha_i)w_i$$

$$= \alpha \sum \alpha_i w_i = \alpha\theta(v)$$

Thusθ is a homomorphism.

Now if v ∈ Ker θ
then θ (v) = **0**

$$\Longrightarrow \theta(\sum \alpha_i v_i) = 0$$

$\Longrightarrow \sum \ \alpha_i w_i = 0 \Longrightarrow$ α_i*=0 for all i* $w_1, w_2, \dots \dots, w_n$*being L.I.*

$\Longrightarrow$ *v=0*$\Longrightarrow$ ker θ $= \{0\} \Longrightarrow \theta$ is one-one
That θ is onto is obvious. Hence θ is an. Isomorphism

Corollary :

Under an isomorphism, a basis is mapped onto a basis

Follows by first part of the theorem.

Problem :

Show that the set of all real valued continuous functions *y= f(x)* sati sing the differential equation$\frac{d^3y}{dx^3} + 6\frac{d^2y}{dx^2} + 11\frac{dy}{dx} + 6y = 0 is\ a$ vector space over **R.** Find a basis of this

Solution :

One can check that $V = \{ f | f\colon \boldsymbol{R} \rightarrow \boldsymbol{R}, f \text{cont.}\}$ is a vector space, over R, under $(f + g)x = f(x) + g(x)$

$$(\alpha f)x = \alpha(f(x))$$

Let $W = \{f \in V | f$ is a solution of given differential equation$\}$

The given differential equation is.

$$(D^3 + 6D^2 + 11D + 6)y = 0$$

$$(D+1)(D+2)(D+3)y = 0$$

$$D = -1, -2, -3$$

and this general solution is

$$y = Ae^{-x} + Be^{-2x} + Ce^{-3x}$$

If S= $\{e^{-x}, e^{-2x}, e^{-3x}\}$ then clearly S spans W

Let $\mathrm{Ae^{-x} + Be^{-2x} + Ce^{-3x} = 0}$

Then$\mathrm{-Ae^{-x} + (-2)Be^{-2x} + (-3D)e^{-3x}}$

$$\mathrm{Ae^{-x}} + (4D)e^{-2x} + (9D)e^{-3x} = 0 \qquad \forall x$$

Put $x = 0$

$$\begin{bmatrix} 1 & 1 & 1 \\ -1 & -2 & -3 \\ 1 & 4 & 9 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0 \Rightarrow M \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0$$

Where

$$\det M = 1(-18+12) - 1(-9+3) + 1\,(-4+2) = -2 \neq 0$$

ThusM^{-1}exists and so $A = B = C = 0$

⇒S is L.I. and hence a basis of$W$. .

Note :

W is a vector space as it is a subspace of V.

$[y_1, y_2, \in \ W \ \Rightarrow \ \alpha_1 y_1 + \alpha_2 y_2$is asolution of the given differential equation $\Rightarrow \alpha_1 y_1 + \alpha_2 y_2$ ∈W].

Problem:

If$S = \{v_1, v_2, \ldots\ldots, v_r\}$is a L.l. subset of V and v ∈ V be such that $v \notin L(S)$, then $S \cup \{v\}$ is a L.I., subset of V.

Solution:

$S \cup \{v\} = \{v_1, v_2, \ldots\ldots, v_r, v\}$

Let $\alpha_1 v_2 + \alpha_2 v_2 + \cdots + \alpha_r v_r + \alpha v = 0 \alpha_i \in F$, $\alpha \in$ F

If $\alpha \neq 0$ then α^{-1} exists and we get

$$\alpha^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_r v_r + \alpha v) = 0$$

$\Rightarrow v = (-\alpha^{-1}\alpha_1)\, v_1 + (-\alpha^{-1}\alpha_2) v_2 + \cdots . + (-\alpha^{-1}\alpha_r) v_r$

⇒ v ∈ L(S), a contradiction

Thus $\alpha = 0$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots. + \alpha_r v_r = 0$

$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2, \ldots.., v_r$ are L.I.

$\Rightarrow \alpha = \alpha_i = 0$for all i.

⇒ $v_1, v_2, \ldots\ldots, v_r$, v are L.I..

Hence the result follows.

Problem:

(1, 1, 1) is L.I. vector in **R^3(R).** Extend it to form a basis of **R^3**.

Solution:

(1, 1, 1)is non zero vector and is therefore L.I. in **R^3**.

Let $S = \{(1,1,1)\}$, then $L(S) = \{\Rightarrow \alpha(l,1,1) | \alpha \notin R\}$

Now $(1,0,0) \in \boldsymbol{R}^3$, but $(1,0,0) \notin L(S)$

thus by above problem $S_1 = \{(1,1,1), (1,0,0)\}$ is L.I.

Now $L(S_1) = \{\alpha(1,1,1) + \beta\,(1,0,0) | \alpha, \beta\ \boldsymbol{R}\}$

$= \{(\alpha + \beta, \alpha, \alpha) \mid \alpha, \beta \in \mathrm{R}\}$

Again $(0,1,0) \notin L(S_1)$ and by above problem

$S_2 = \{(1,1,1), (1,0,0), (0,1,0)\}$ is L.I. subset of **R^3**Since dim **R^3** = 3,we find S_2 will be a basis of **R^3**.

Problem:

A finite set of non zero vectors $\{v_1, v_2, \ldots.., v_n\}$ in a vector space V(F) is L.D. iff$\exists v_k$, $2 \leq k \leq n$, s.t., v_k is a linear combination of $v_1, v_2, \ldots.., v_{k-1}$.

Solution:

Letv_1,v_2,…..,v_n be L.D. Then $\exists\alpha_i \in$ F, not all zero s.t

$$\sum_{i=1}^{n} \alpha_i v_i = 0$$

Let k be the largest integer s.t $\alpha_k \neq 0$
then k≠1 as if k = 1,
then $\alpha_1 v_1$=0 ,$\alpha \neq 0(\alpha_i = 0\ for\ all\ i \geq 2) \Longrightarrow v_1$=0 , not true as v_i are non zero. Hence , $2 \leq k \leq n$
thus $\alpha_i \neq 0$ and $\alpha_i = 0$for all i ≥ $k + 1$. Also then $\alpha_k{}^{-1}$l exists
$\Longrightarrow \alpha_1 v_1$+$\alpha_2 v_2$+…….+$\alpha_k v_k$ =0
$\Longrightarrow \alpha^{-1}{}_k(\alpha_1 v_1$+$\alpha_2 v_2$+……+$\alpha_k v_k$)=0
$\Longrightarrow v_k$= $(-\alpha_k{}^{-1}\alpha_1)v_1$+$(-\alpha_k{}^{-1}\alpha_2)v_2$+…….+$(-\alpha_k{}^{-1}\alpha_{k-1})\alpha_{k-1}$
which proves the result.
Conversely, suppose $\exists k$, , $2 \leq k \leq n$ s.t v_k is a linear combination of v_1,v_2,…..,v_{k-1}.
Let $v_k = \alpha_1 v_1$+$\alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1} \alpha_i \in F$
Then $\alpha_1 v_1$+$\alpha_2 v_2 + \cdots + \alpha_{k+1} v_{k+1} - 1.v_k$ =0
$\Longrightarrow v_1$,v_2,…..,$v_k$are L.D. as $(-1) \neq 0$
$\Longrightarrow v_1$,v_2,…..,v_k,v_{k+1},……,v_n are L.D. as any super set of a L.D. set is L.D. Hence the result follows.

Theorem(2.32):

Let W be a subspace of a F.D.V.S. V, then W is finite dimension and dim $W \leq dim\ V$. In fact, dim$V = dim\ W$ iff $V = W$.

Proof :

Let $dimV = n$, then n is the maximum number of L.I. elements in any subset of V. Since any subset of W will be a subset of V , n is the maximum number of L.I. elements in W.
Let w_1,w_2,…..,w_m, be the maximum number of L.L elements inW then $m \leq n$
We show $\{w_1$,w_2,…..,$w_m\}$ is a basis of W. These are already L.I.
If w∈ W beany element then the set $\{w_1$,w_2,…..,w_m,w$\}$ is L.D.
$\Longrightarrow \exists\alpha_1$,$\alpha_2$,…..,$\alpha_n$, α in F (not all zero) s.t
$\alpha_1 w_1$+………+$\alpha_m w_m + \alpha w$ =0.
If α=0 ,we get α_i= 0 for all i as w_1,……,w_m are L.L. which is not true
Thus α ≠0and so α^{-3} exists.
The above equation then gives us
w = $(-\alpha^{-1}\alpha_1)\ w_1 + \cdots + (-\alpha^{-1}\alpha_m)\ w_m)$
Showing that $\{w_1, w_2, \ldots, w_m\}$ spans W (and thus w is finite dimensional) $\Longrightarrow$ $\{w_1$,w_2,…..,$w_m\}$ is a basis of W $\Longrightarrow dim\ w = m \leq n = dim\ V$ Finally, if $dim\ V = dim\ W = n$ and $\{w_1$,w_2,…..,$w_m\}$ be .a basis of W then as $\{w_1$,w_2,…..,$w_m\}$ is

L.I. in W, it will be L.I. in V.
and as dim V= n, $\{w_1,w_2,\ldots.,w_m\}$ is a basis of V. Now if v ∈ V be any element the v = $\alpha_1 w_1+\alpha_2 w_2+\ldots\ldots+\alpha_n w_n \in W$
$\Rightarrow$ v $\subseteq W \Rightarrow$ V =W
Conversely, of course, $V = W \Rightarrow dim\, V = dim\, W.$

Remark:

If W is a subspace of V where $W = (0)$ then dimension of W is taken to be zero .

Theorem (2.33):

LetW be subspace of a F.D.V.S.V then

$$\dim \frac{V}{W} = \dim V - \dim W$$

Proof:

Let $\dim W = m$and let $\{w_1, w_2, \ldots, w_m\}$ be a basis of W . $w_1, w_2, \ldots, w_m$ being L.I in W will be L.I in V and thus $\{w_1, w_2, \ldots, w_m\}$ can be extended to form a basis of V .

Let $\{w_1, w_2, \ldots, w_m, v_1, v_2, \ldots, v_n\}$ be the extended basis of. V then

$$\dim V = n + m$$

Consider the set $= \{W + v_1, W + v_2, \ldots, W + v_n\}$, we show it form a basis of $\frac{V}{W}$

Let $a_1(W + v_1) + \cdots + a_n(W + v_n) = W, a_i \in F$ then

$$W + (a_1 v_1 + \cdots + a_n v_n) = W \Rightarrow a_1 v_1 + \cdots + a_n v_n \in W$$
$$\Rightarrow a_1 v_1 + \cdots + a_n v_n \text{is a linear combination of} w_1, \ldots, w_m$$
$$\Rightarrow a_1 v_1 + \cdots + a_n v_n = \beta_1 w_1 + \cdots + \beta_m w_m \beta_j \in F$$
$$\Rightarrow a_1 v_1 + \cdots + a_n v_n - \beta_1 w_1 - \cdots - \beta_m w_m = 0$$
$$a_i = \beta_i = 0 \text{ for all } i, j$$
$$\Rightarrow \{W + v_1, W + v_2, \ldots, W + v_n\} \text{is L.I}$$

Again for any $, v \in \frac{V}{W}$, v$\in V$ means v is a linear combination of $w_1, w_2, \ldots, w_m, v_1, v_2, \ldots, v_n$

i.e$a_1 w_1 + \cdots + a_m w_m + \beta_1 v_1 + \cdots + \beta_n v_n a_i, \beta_j \in F$

again $W + (a_1 w_1 + \cdots + a_m w_m) + (\beta_1 v_1 + \cdots + \beta_n v_n)$

$$= W + (\beta_1 v_1 + \cdots + \beta_n v_n)$$
$$= \beta_1(W + v_1) + \cdots + \beta_n(W + v_n)$$

Hence s space $\frac{V}{W}$ and is therefore a basis dim $\frac{V}{W} = 0$ thus

$$\dim \frac{V}{W} = \dim V - \dim W$$

Theorem (2.34):

If A and B are two subspace of a F.D.F.S. V then

$$\dim(A + B) = \dim A + \dim B - \dim(A \cap B).$$

Proof :

We have already proved that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$
$$\dim \frac{A+B}{A} = \dim \frac{B}{A \cap B}$$
$$\Longrightarrow \dim(A+B) - \dim A = \dim B - \dim(A \cap B)$$

Or the $\dim(A+B) = \dim A + \dim B - \dim(A \cap B)$

Remark:

The reader should try to give an independent proof of the above theorem an exercise .

Corllory :

If $A \cap B = (0)$ then $\dim(A+B) = \dim A + \dim B$

$$\dim(A \oplus B) = \dim A + \dim B$$

Problem:

Le $p_n$be the vector space of all polynomial of $degree \leq n$ over R exibit a basis of $\frac{\mathrm{P}_4}{\mathrm{P}_2}$. hence verify that $\dim \frac{\mathrm{P}_4}{\mathrm{P}_2} = \dim \mathrm{P}_4 - \dim \mathrm{P}_2$.

Solution:

It is easy to see $\{1, x, x^2, x^3, x^4\}$ is a basis of P_4 and thus $\dim \mathrm{P}_4 = 5$. Similarly $\dim \mathrm{P}_2 = 3$ as $\{1, x, x^2\}$ will be a basis of P_2.

Let $S = \{\mathrm{P}_2 + x^3, \mathrm{P}_2 x^4\}$ then S is a basis of $\frac{\mathrm{P}_4}{\mathrm{P}_2}$ as

$$\mathrm{P}_2 + f \in \frac{\mathrm{P}_4}{\mathrm{P}_2} \Longrightarrow \mathrm{P}_2 + a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 = \mathrm{P}_2 + f$$
$$\Longrightarrow \mathrm{P}_2 + f = a_3(\mathrm{P}_2 + x^3) + a_4(\mathrm{P}_2 + x^4)$$
$$\Longrightarrow S \text{ spans } \frac{\mathrm{P}_4}{\mathrm{P}_2}$$

Again $\quad a(\mathrm{P}_2 + x^3) + \beta(\mathrm{P}_2 + x^4) = \text{zero} = \mathrm{P}_2$

$$\Longrightarrow \mathrm{P}_2 + a x^3 + \beta x^4 = \mathrm{P}_2$$
$$\Longrightarrow a x^3 + \beta x^4 = a + bx + cx^2 \in \mathrm{P}_2$$

$\Longrightarrow a = b = c = \alpha = \beta = 0$ as polynomial is zero , if each coefficient is zero thus S is a basis of $\frac{\mathrm{P}_4}{\mathrm{P}_2}$

Hence $\dim \frac{\mathrm{P}_4}{\mathrm{P}_2} = 2 = 5 - 3 = \dim \mathrm{P}_4 - \dim \mathrm{P}_2$

Theorem (2.35):

Let W be a subspace of F.DV.S. V , then there exists a subspace W' of V such that $V = W \oplus W'$.

Proof :

Let $\{w_1, w_2, \dots, w_m\}$ be a basis of W , then $w_1, w_2, \dots, w_m$ being L.I in W will be L.I in V. we extend these L.I elements to form a basis of V , say $\{w_1, w_2, \dots, w_m, v_1, v_2, \dots, v_n\}$

Let $W' = L(\{v_1, v_2, \dots, v_n\})$, i.e., W' be the subspace spanned by $\{v_1, v_2, \dots, v_n\}$

We show $W \oplus W' = V$,Let $v \in$ V be any element, then

V = $(\alpha_1 w_1 + \cdots + \alpha_m w_m) \; + \; (\beta_1 v_1 + \cdots + \beta_n v_n), \quad \alpha_i, \beta_i \in \; F$
where the first bracket term belongs to W and the second to W' and the second to W'

$\therefore \; v \in \; W + W'$ and thus $V \subseteq \; W \; + \; W'$

$$\Longrightarrow V \; = W + W'$$

Again, if $x \; \in \; W \cap \; W'$ be any element
then $x \in \; W$ and $x \; \in \; W'$

$$\Longrightarrow \; x \; = \; \alpha_1 w_1 + \cdots . + \alpha_m w_m \alpha_i, b_j \in \; F$$

$$x \; = \; b_1 v_1 + \cdots + b_n v_n$$

$\Rightarrow \alpha_1$w$_1$+ .... +$\alpha_m w_m$ + $(-$b$_1)$v$_1$ +......+$(-$b$_n) v_n$ = 0

$\Rightarrow \alpha_i$=b$_j$=0 for all i, j w$_1$,….,w$_m$, v$_1$,…., v$_n$ being L.I.

Hence $x = 0$

$$W \cap W' = \; (0)$$

or that $V = \; W \oplus W'$

Note :

W' is called complement of W. Thus we have proved that every subspace of a F.D. V.S. has a complement.

Corllory :

If W' is any complement of W in V then $dimW' \; = \dim V - \dim W$

. Since $V \; = \; W \oplus W' \; \Rightarrow \dim V = \dim(W \oplus W') = \dim W + \dim W'$

$= \; dimW' \; = \dim V - \dim W.$

Although every complement of a subspace has same dimension it does not mean. that a subspace has a unique complement.
Consider

Example :

Let $V \; = \; R^2(R) and \; let$
W = {(α,0)|α ∈**R**}
W_1= {(0,b)|b∈ ***R***}

$$W_2 = \{(c, c) | c \in \boldsymbol{R}\}$$

it is easy to see that W,W_1,W_2 are subspaces of V
We show V = W ⊕ W_1 and V = W ⊕ W_2

Now $\quad v \; \in \; V \; \Longrightarrow v = \; (x, y) = \; (x, 0) + \; (0, y) \in \; W \; + \; W_1$

$$\Rightarrow V \; \subseteq W + W_1 \; \Rightarrow \; V = W + W_1$$

again $x \; \in W \cap W1 \; \Rightarrow \; x \in \; W \; and \; x \in \; W_1$

$$\Rightarrow \; x \; = \; (a, 0), x = (O, b)$$

$$\Rightarrow (a, 0) = (0, b) \Rightarrow \; a = b = O \; \; \Rightarrow x = O$$

Hence $\quad W \cap W_1 \; = \; (0)$
or that V =W⊕ W_1.

Also $v \in \; V \; \Rightarrow \; \; v \; = \; (x, y) = \; (x \; - \; y, \; 0) \; + \; (y, y) \; \in \; W \; + \; W_2$

$$\Rightarrow V \subseteq W + W_2 \Rightarrow V = W + W_2$$

Now $x \in W \cap W_2 \Rightarrow x \in W \; and \; x \in W_2 \Rightarrow \quad x = (a, 0), x = (c, c) \Rightarrow (a, 0) = (c, c) \Rightarrow c = 0, \Rightarrow x = (0,0)$.

Thus W∩ W_2=(O) or that $V = W \oplus W_1$.

.: Notice that W, W_1,W_2,are spanned by $\{(1;\; 0)\}, \{(0, 1)\}, \{(l, l)\}$ respectively d as each of these is L.I. (they are non zero). These subsets form bases of W,W_1,W_2 respectively.

Hence $dim\, W = dim\, W_1 \; dim\, W_2 = 1$.

Inner Product Spaces

In general a vector space is defined over an arbitrary field F and this is what We did earlier . In this' section .we restrict F the field of real or complex numbers. In the first case, the vector space is called real vector space and in the second case it is called a complex vector space. We study real vector spaces in analytical geometry and vector analysis. There we discuss the concept of length and orthogonality. We also have dot or scalar product of two vectors which among other things satisfies the following

(i) $\vec{v}.\vec{v} \geq 0$ and $(\vec{v}.\vec{v}) = 0 \Leftrightarrow \vec{v} = 0$

(ii) $\vec{v}.\vec{w} = \vec{w}.\vec{v}$

(iii)$\vec{v}$.$(\alpha\vec{v} + \beta\vec{v}) = \alpha(\vec{u}.\vec{v}) + \beta(\vec{u}.\vec{w})$

where $\vec{u}, \vec{v}, \vec{w}$ are vectors and $\alpha\beta$ real numbers .We wish to extend the concept of dot product to complex vector spaces also. We define a map on $V \times V$ of (where *V*= vector space over *F)* with same property as dot product, called inner product and study the concept of length and orthogonality.

Def(2.36) :

Let *V* be a vector space over field *F* (where *F* = field of real or complex numbers). Suppose for any two vectors *u, v* ∈ *V* ∃ an element $(u, y) \in F \; s.t$ [(u, v)here is just an element of *F* and should not be confused with the ordered pair.]

(i) $(u, v) = \overline{(v, u)}$(i.e .,comblex conjugate of (v, u))

(ii) $(u, u) \geq 0 \; and \; (u, u) = 0 \Leftrightarrow u = 0$

(iii) $(\alpha u + \beta v, w) = \alpha(u, w) + \beta(\boldsymbol{v}, w)$

for any $u, v, w \in V$ and $\alpha, \beta \in$ F.
Then V is called an inner product space and the function satisfying (i), (ii) and., (iii) is called an inner product. Thus inner product space is a vector space over the field of real or complex numbers with an inner product function.

Remarks :

1. Property (ii) in the definition of inner product space makes sense in as much as $(u, u) = \overline{(u, u)}$by (i) ⇒ (u, u) = real.
2. Property (iii) can also be described by saying that inner product is a linear map in 1st variable.
3. Can we say that inner product is linear in and variable?

Let's evaluate

$$(u, \alpha v + \beta w)\overline{(\alpha v + \beta w, u)} \quad by\ (i)$$

$$= \overline{\alpha}\overline{(v, u)} + \overline{\beta}\overline{(w, u)}$$

$$= \overline{\alpha}\ (u, v) + \overline{\beta}\ (u, w)$$

So, it need not be linear in 2nd variable.

1. If F =field of real numbers, then the function inner product satisfies same properties as dot product seen earlier.

2. Inner product space over real field is called Euclidean space and over complex field is called Unitary space.

Example:
Let V = $R^{(2)}$, u = $(\{\alpha_1\ , \alpha_2)\ v = (\beta_1\ , \beta_2)$.

Defin $(u, v) = \alpha_1\beta_1 - \alpha_2\beta_1 - \alpha_1\beta_2 + 4\alpha_2\beta_2$
Then

(i) $(u, v) = (v, u) = \overline{(v, u)}$

(ii) $(u, u) = (\alpha_1 - \alpha_2)^{\ 2} + 3\alpha_2^2 \geq 0$
$(u, u) = 0 \Leftrightarrow \alpha_1 = \alpha_2, \alpha_2 = 0 \Leftrightarrow \alpha_1 = 0 = \alpha_2$
$\Leftrightarrow u = (\alpha_1 - \alpha_1) = (0, 0) = 0$
(iii) $(\alpha u + \beta u, w) = \alpha(u, w) + \beta(v, w)$
can be easily verified. Thus, (u, v) defines an inner product.

Example:

Let ,W_1 , W_2 be two subspaces of a vector space V If W_1 , W_2 are inner product spaces, show that $W_1 + W_2$ is also an inner product space.

Solution:

Let $x. y \in W_1 + W_2$.

Then $x = u_1 + u_2$

$y = v_1 + v_2 u_1 , v_1 \in W_1 ; u_1, v_2 \in W$

Define $< x, y > = (u_1, v_1) + (u_2, v_2)$

Then x=u_1 + u_2

y = v_1+v_2 , u_1 ,v_1 ∈W_1 , $u_2, v_2 \in W_2$

Define $< x, y >$ = (u_1 ,v_1)+(u_2, v_2)

Then

(i) $\overline{< y, x >} = \overline{(v_1, u_1) + (v_2, u_2)}$

$= \overline{(v_1, u_1)} + (\overline{(v_2, u_2)}$

=(u_1 ,v_1)+(u_2, v_2)= < x, y>

(ii) $< x, x >$=(u_1,u_1) + (u_2,u_2) ≥ 0 And $< x , x > = 0 \Leftrightarrow$ (u_1,u_1) = 0 = (u_2,u_2)$\Leftrightarrow u_1 = 0 = u_2 \Leftrightarrow x = 0$

(iii) $< \alpha x + \beta y, z > = \alpha < x, z > + \beta < y, z >$ can be easily verified.

∴$< x, y >$ defines an inner product on $W_1 + W_2$

So , $u_1 + u_1$ *is* an inner product space .

Norm of a vector

Let V be an inner product space. Let v ∈ V. Then norm of v (or length of v) defined as $\sqrt{(v, v)}$ and is denoted by ||v||.

Problem:

||αv|| = |α| ||v|| for all α ∈ F, v∈ V

Solution:

$\left||\alpha v|\right|^2$ =(αv, αv)= $\alpha\overline{\alpha}(v, v)$ =$|\alpha|^2||\alpha||^2$ ⇒ $\left||\alpha v|\right| = |\alpha| \; ||v||$

We now prove an important inequality known as Cauchy Schwarz inequality

Theorem(2.37):

Let V be an inner product space.

Then $|(u,v)| \leq ||u|| \; ||v||$ for all u ,v ∈ V

Proof :

If $u = 0$, then $(u, v) = (0, v) = 0$ and $||u|| = \sqrt{(u\,, u)} = \sqrt{(0,0)} = 0$

$\therefore$ LH.S. = R.H.S.

Let u ≠ 0. Then ||u|| ≠ 0

(as $||u|| = 0 \Rightarrow \sqrt{(0,0)} = 0 \Rightarrow (u, u) = 0 \Rightarrow u = 0$)

$$Let \quad W = \frac{(u, v)}{||u||^2} u$$

Then $(w,\ w) = \left[\frac{(u,v)}{||u||^2}\, u\,, v - \frac{(v,\ u)}{||u||^2}\ u\right]$

$$= (u, v) - \frac{(v,\ u)}{||u||^2}(u, v)$$

$$= ||v||^2 \frac{\overline{(u, v)}(u, v)}{||u||^2} \quad = ||u||^2 - \frac{|(u, v)|^2}{||u||^2}$$

$$= \frac{||u||^2 ||v||^2 - |(u, v)|^2}{||u||^2}$$

Since $(w,\ v) \geq 0. |(u,\ v)|^2 \leq ||u||^2 ||v||^2$

$$|(u, v)| \leq \ ||u|| ||v||.$$

Remark :

The above inequality will be an equality if and only if

Proof:

suppose $|(u, v)| ||u|| ||V||$

If $u = 0$, then $u = 0$, $v \Longrightarrow$ $u,\ v$ are linearly dependent. Let u ≠ 0. Then from above

$$(w,\ w) = 0 \ \Longrightarrow w \ = 0$$

$$V \ - \frac{(v,\ u)}{||u||^2} u \ \ = 0$$

$$\Longrightarrow v \ = \frac{(v,\ u)}{||u||^2}\ u \Longrightarrow u, v\ are\ linearly\ dependent.$$

Conversely , Let u = av , $a \in F$

Then $|(u,\ v)| \ = |a\ (v\,, v)| = |\ a\ ||| \ v\ ||^2$

$||\ u\ |||| \ v\ || = |a\ ||| \ v\ |||| \ v\ || = |a\ ||| \ v\ ||^2 |(u, v)| = \ ||\ u\ |||| \ v\ ||$

Theorem(2.38) :

Let V be an inner product space. Then

(i)$||x + y|| = ||x|| + ||y||$ for all $x, y \in V$

(Triangle inequality)

(ii) $||x + y||^2 + ||x - y||^2 = 2(||x||^2 + ||y||^2)$(parallelogram law)

Proof:

(i)$\|x+y\|^2 = (x+y, x+y)$

$$= (x,x) + (y,x) + (x,y) + (y,y)$$
$$= \|x\|^2 + \overline{(x,y)} + (x,y) + \|y\|^2$$
$$= \|x\|^2 + 2Re(x,y) + \|y\|^2$$
$$\leq \|x\|^2 + 2|(x,y)| + \|y\|^2$$
$$\leq \|x\|^2 + 2\|x\|^2\|y\|^2 + \|y\|^2$$
$$= (\|x\|^2 + \|y\|^2)^2$$

Hence $\|x+y\| \leq \|x\| + \|y\|$

This is called triangle inequality as$\|x\|^2 + \|y\|^2 =$ sum of the lengths of two sides of a triangle

$\|x+y\| =$ length of the third side of the triangle showing that sum of two of a triangle is less than. its third side.

(ii)$\|x+y\|^2 + \|x-y\|^2 = (x+y, x+y) + (x-y, x-y) =$ $\|x\|^2 + \|y\|^2 + (x,y) + (y,x) + \|x\|^2 + \|y\|^2 - (x,y) -$ $(y,x) = 2(\|x\|^2 + \|y\|^2)$

Note :

$\|x+y\|^2 + \|x-y\|^2 =$ sum of squares of lengths of diagonals a parallelogram

$2(\|x\|^2 + \|y\|^2) =$ sum of squares of sides of a parallelogram.

∴sum of squares of lengths of diagonals of a parallelogram is equal to sum of squares of lengths of its sides. For this reason (ii) is called parallelogram law.

Problem:

Using Cauchy Schwarz inequality, prove that cosine of an angel is of absolute vale at most 1.

Solution:

Let F = field of real numbers and V = F (3)

Consider standard inner product on V.

Let $u = (x_1, y_1, z_1)$, $v = (x_2, y_2, z_2) \in F, O = (0,0,0)$

Let θ be an angle between OU and OV.

Then

$$\cos\theta = \frac{x_1x_2 + y_1y_1 + z_1 + z_2}{\sqrt{x_1^2 + y_1^2 + z_1^2}\sqrt{x_2^2 + y_2^2 + z_2^2}} = \frac{(u,v)}{\|u\|\|v\|}$$
$$|\cos\theta| = \frac{(u,v)}{\|u\|\|v\|} \leq \frac{\|u\|\|v\|}{\|u\|\|v\|} = 1$$

Orthogonality

Let *V* be an inner product space. Two vectors $u, v \in V$are said to be orthogonalif $(u,v) = 0 \Leftrightarrow (v,u) = 0$. So, *u* is orthogonal to *v iff v* is orthogonal to *u.* Since $(0,v) = 0$ for all $v \in V$, 0 is orthogonal to every vector in *V.*

Conversely ,if $u \in V$is orthogonal to every vector in V then $(u, v) = 0 \Rightarrow u = 0$. Let W be a subspace of V.
Define $W^{\perp} = \{v \in V \mid (v, w) = 0$ for all $w \in W(W^{\perp}$is read as W perpendicular).
Then $W^{\perp}$is a subspace of Vas $0 \in W^{\perp} \Rightarrow W^{\perp} \neq \varphi$and

$(a\mathrm{v}_1 + \beta v_2\, , w) = a(\mathrm{v}_1, w) + \beta(\mathrm{v}_2, w) = 0$ for all $w \in W$

$$\Rightarrow a\mathrm{v}_1 + \beta\mathrm{v}_2 = W^{\perp}$$

$W^{\perp}$is called orthogonal complement of W. The reason for calling it thus is because we shall prove later that $V = W \oplus W^{\perp}$

Problem:

Let V be an inner product space. *Let $x, y \in V$ s.t. $x \perp y$ Then show that*$\|x + y\|^2 = \|x\|^2 + \|y\|^2$(This is Pythagoras Theorem when *F=R as in triangle ARC with* $AB \perp BC, AB^2 = \|x\|^2, BC^2 = \|y\|^2, AC^2 l = \|x + y\|^2$)

Solution:

$$\|x + y\|^2 = (x + y, x + y) = (x, x) + (y, y) + (x, y) + (y, x)$$

$= \|x\|^2 + \|y\|^2$ as $(x, y) = 0 = (y, x)$

Orthonormal Set

A set $\{u_i\}_i$of vectors in an inner product space V is said to be orthogonal if $(u_i, u_j) = 0\; for\; i \neq j$.If further $\left(u_i, u_j\right) = 1$ for all *i* then the set $\{u_i\}$is called an *orthonormal set.*

Example:

Let V be the real vector space of real polynomials of degree less than or equal to *n.* Define an inner product on V by

$$\left[\sum_{i=1}^{n} a_i x^i\, , \sum_{j=1}^{n} b_j x^i\right] = \sum_{1}^{n} a_i b_j$$

Then $\{\, 1, x, \ldots\, , x^n\}$ is an orthonormal subset of V.

Theorem (2.39):

Let S be an orthogonal set of non zero vectors in an inner product space V. Then S is a linearly independent set.

Proof :

To show S is linearly independent, we have to show that every finite subset of S is linearly independent.
Let $\{v_1, \ldots, v_n\}$ be a finite subset of S.
Let $a_1 v_1, \ldots, a_n v_n = 0\, , a_i \in F$

$$(a_1v_1 + \cdots + a_nv_n\,, a_1v_1, \ldots, a_nv_n) = 0$$

$$\Longrightarrow |a_1|^2\|v_1\|^2 + \cdots + |a_n|^2\|v_n\|^2 = 0$$

$\Longrightarrow |a_i|^2\|v_i\|^2 = 0$ *for all i=1,…n*

$\Longrightarrow |a_i|^2 = 0$ *for all I I as* $\|v_i\|^2 = 0 \Longrightarrow \|v_i\| \quad = 0 \Longrightarrow \mathrm{v_i} = 0$

Which is not true

$\Longrightarrow a_i = 0$ *all i=1,…,n*
⟹S is linearly independent.
Corllory:
An orthonormal set in an inner product space is linearly independent
Proof:
Let S be an orthonormal set in an inner product space *V*. Let $v \in S$,then $v \neq 0\ as\ v = 0 \Longrightarrow (v, v) = 0 \neq 1$, a contradiction. Therefore, S is an orthogonal set of non zero vectors and so linearly independent.
Theorem (2.40):
(Gram-Schmidt Orthogonalistion process)
Let V be a nonzero inner product space u/dimension n. Then V has an orthonormal basis.
Proof :
It is enough to construct an orthogonal basis .of *V*. For let $S \subseteq V$ be orthogonal set. Then $T = \left\{\frac{x}{\|x\|} | x \in S\right\}$ a is an ortlnorma1 set.
Let $\{v_1, \ldots, v_n\}$be a basis of *V*.
Let $\mathrm{w_1} = \mathrm{v_1}$Define $\mathrm{w_2} = \mathrm{v_2} - \frac{(\mathrm{v_2},\mathrm{w_1})}{(\mathrm{w_1},\mathrm{w_1})}\mathrm{w_1}$

$$= \mathrm{v_2} - \frac{(\mathrm{v_2}, \mathrm{v_1})}{(\mathrm{v_1}, \mathrm{v_1})}\mathrm{v_1}$$

then $\qquad (w_2, w_1) = (w_2, v_1)$

$$(v_2, v_1) = \frac{(\mathrm{v_2}, \mathrm{v_1})}{(\mathrm{v_1}, \mathrm{v_1})}(v_1, v_1) = 0$$

Also $\qquad v_2 = a_1v_1 + w_2 = a_1w_1 + w_2$

Where $\quad a_1 = \frac{(\mathrm{v_2},\mathrm{v_1})}{(\mathrm{v_1},\mathrm{v_1})} \in F$
Note $\mathrm{v_1}$, is linearly independent $\mathrm{v_1} \neq 0 \Longrightarrow (\mathrm{v_1}, \mathrm{v_1}) \neq 0)$
Define $\mathrm{w_1} = \mathrm{v_3} - \frac{(\mathrm{v_3},\mathrm{w_1})}{(\mathrm{w_1},\mathrm{w_1})}\mathrm{w_1} - \frac{(\mathrm{v_3},\mathrm{w_1})}{(\mathrm{w_1},\mathrm{w_1})}w_1$

Then $(w_3, w_2) = 0 = (w_3, w_1)$
Also where
In this way, we can construct an orthogonal set $\{w_1, \dots, w_n\}$ where each

$$v_i = a_1 w_1 + \cdots + w_i \ , \quad a_i \in F$$

$\therefore \left\{\frac{w_1}{||w_1||}, \dots \dots, \frac{w_n}{||w_n||}\right\}$ is an orthonormal set which is linearly independent by

Problem :
Obtain an orthonormal basis, w.r.t. the standard inner product for the subspace of $\boldsymbol{R^3}$ generated by (1,0,3) and (2,1,1).

Solution:
Let v_1 = (1, 0, 3), v_1= (2, 1, 1) .

Then w_1=v_1, $w_2 = v_2 - \frac{(v_1,w_1)}{(u_1,u_1)} w_1$
Now (w_1, w_1) = (v_1 , v_1) = 2+ 0 + 3=5

$$(w_1, w_1) = (v_1 , v_1) = 1 + 0 + 9 + 10$$

$\therefore$ $||w_1||$ = $\sqrt{10}$

So , $w_2 = (2,1,1\,) - \frac{5}{10}\,(1,0,3\,) = \left(\frac{3}{2}, 1\,, \frac{1}{2}\right)$

$$\therefore \ ||w_2|| = \sqrt{\frac{9}{4} + 1 + \frac{1}{4}} = \sqrt{\frac{7}{2}}$$

$\therefore$ required orthonormal basis is

$$\left\{\frac{w_1}{||w_1||}, \frac{w_2}{||w_2||}\right\} = \left\{\frac{1}{\sqrt{10}}(1,0,3), \frac{\sqrt{2}}{7}\left(\frac{\sqrt{3}}{2}, 1, -1\right)\right\}$$

Theorem(2.41): (Bessel's inequality)

If $(w_1\,, w)$ is an orthonormal set in V. then

$$\sum_{i=1}^{m} |(w_i, v)|^2 \le ||v||^2 \quad for\ all\ \ v \in V$$

Proof :

Let $x = v - \sum_{i=1}^{m}(v, w_i)w_i$
$(x, w_j) = (v, w_j) - (v, w_j) = 0$ for all $j = 1, \dots, m$. Let

$$w = \sum_{i=1}^{m}(v, w_i)w_i = \sum_{i=1}^{m} a_i w_i \, , a_i = (v, w_i)$$

$\therefore \quad v = x + w$

Also

$$(w, x) = (a_1 w_1 + \cdots + a_m w_m \, , x)$$
$$= a_1(w_1, x) + \cdots + a_m(w_m \, , x) = 0$$

Now $\|v\|^2 = (v, v)$

$$= (w + x \, , w + x) = (w, w) + (x, x) = \|w\|^2 \|x\|^2 \geq \|w\|^2$$

But $\|w\|^2 = (w, w)$

$$= (a_1 w_1 + \cdots + a_m w_m \, , a_1 w_1 + \cdots + a_m w_m)$$

$$= a_1 \overline{a_1}(w_1 \, , w_1) + \cdots + a_m \overline{a_m}(w_m \, , w_m)$$

$$= |a_1|^2 + \cdots + |a_m|^2$$

as $\{w_1 \, , \dots , w_m\}$ is an orthonoal set

$$\sum_{i=1}^{m}|a_i|^2 = \sum_{i=1}^{m}|(v, w_i)|^2 = \sum_{i=1}^{m}\left|\overline{(w_\imath \, , v)}\right|^2 = \sum_{i=1}^{m}|(w_i \, , v)|^2$$

$\therefore \quad \sum_{i=1}^{m}|(w_i \, , v)|^2 \leq \|v\|^2 \quad for\ all\ \|v\|^2\ v \in V$

Corllory:

Equality holds if and only if $v = w$

Proof:

Suppose $v = w$

Then

$$\|v\|^2 = \|w\|^2 = \sum_{i=1}^{m}|(w_i \, , v)|^2$$

conversely ,suppose equality holds . then

$$\|v\|^2 = \|w\|^2 \Longrightarrow \|x\|^2 = 0 \Longrightarrow (x, x) = 0 \Longrightarrow 0$$
$$\Longrightarrow v = w + x = w$$

Fields play an important role algebra with applications to Number theory of equations and geometry .

Def(3.1):

Let L be a field and suppose K is a subfield od F, then K is called an extension of F .

Suppose S is a non empty subset of K, let F(S) denote the smallest subfield of K which contains both f and s .(in fact F(S) would be the inter section of all subfields of K that contain F and S f and s.)

The following theorem is then an easy consequence .

Theorem (3.2):

If S,T are non empty subset of afield k and K is an extension of afield F then $F(S\cup T)=F(S)(T)$ (Where of course , if F(S)=E , then by F(S)(T) we men E(T)

Proof:

$F(S\cup T)$ is the smallest subfield of k containing $(S\cup T),F$

i.e $S,T,F\subseteq F(S\cup T)\Rightarrow F(S)\subseteq F(S\cup T)\ ,\quad T\subseteq F(S\cup T)$

$$\Rightarrow F(S)(T)\subseteq F(S\cup T)$$

again $F,S,T\subseteq F(S)(T)\Rightarrow F,S\cup T\subseteq F(S)(T)$

$$\Rightarrow F(S\cup T)\subseteq F(S)(T)$$

or that $F(S\cup T)=F(S)(T)$

Remark:

If s is finite subset $\{a_1,a_2,\dots,a_n\}$K we write $F(S)=F(a_1,a_2,\dots,a_n)$.

The order in which $a_i$appear is immaterial in view of the next lemma as

$$F(a_1,a_2,\dots,a_n)=F(\{\boldsymbol{a_i}\}\{a_1,a_2,\dots,a_n\})=F(\{a_2,a_3,\dots,a_n\})$$
$$=F(a_2,a_3,\dots,a_n,a_1)$$

Also then

$$F(a)(b)=F(a,b)=F(b,a)=F(b)(a)$$

Again if $K=F(a)$ k is called simple extension of F and we say K is got by adjoining the element a to F.

Lemma (3.3):

$F(S\cup T)=F(T\cup S)=F(S)(T)$ follows clearly as $S\cup T=T\cup S$.

Problem:

Let Q be the field of rationales then show that $Q(\sqrt{2},\sqrt{3})=Q(\sqrt{2}+\sqrt{3})$.

Solution :

By definition

$\sqrt{2},\sqrt{3}\in Q(\sqrt{2},\sqrt{3})\Rightarrow\sqrt{2}+\sqrt{3}\in Q(\sqrt{2},\sqrt{3})$ (closure)

$$\Rightarrow Q(\sqrt{2}+\sqrt{3})\subseteq Q(\sqrt{2},\sqrt{3})$$

Now $\sqrt{2}+\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})\Rightarrow(\sqrt{2}+\sqrt{3})^2\in Q(\sqrt{2}+\sqrt{3})$

Also 5 $\in Q(\sqrt{2}+\sqrt{3})$

$$5+2\sqrt{2}\sqrt{3}-5=2\ ,\ \sqrt{2}\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$$

Also $2\in Q\left(\sqrt{2}+\sqrt{3}\right)$

$$2\times\frac{1}{2}\sqrt{2}\sqrt{3}=\sqrt{2}\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$$

Also $\sqrt{2}+\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$

$$\Longrightarrow 3\sqrt{2}+3\sqrt{3}-2\sqrt{3}-3\sqrt{2}=\sqrt{3}\in Q(\sqrt{2}+\sqrt{3})$$

$$\Longrightarrow 2\sqrt{3}+3\sqrt{2}-2\sqrt{2}-\sqrt{3}=\sqrt{2}\in Q(\sqrt{2}+\sqrt{3})$$

$$\therefore Q(\sqrt{2},\sqrt{3})\subseteq Q(\sqrt{2}+\sqrt{3})$$

$$\therefore Q\left(\sqrt{2},\sqrt{3}\right)=Q(\sqrt{2}+\sqrt{3})$$

If k is an extension of F, then we know that K can be regarded as a vector space over F. in that case dimension of K over F is called degree of K over F and we denote it by [K:F].

Our next theorem is about the degree of extension fields. If [K:L]is finite ,we say k is finite extension of F.

Theorem (3.4):

Let L be a finite extension of K and F, a finite extension of K . then L is a finite extension of F and [L:F]:[L:K][K:F].

Proof:

Let [L:K]=m , [K:F]=n

Let $\{a_1,\dots,a_m\}$ be a basis of L over K and $\{b_1,\dots,b_n\}$be be a basis of k over F. we show that $\{a_ib_j|1\le i\ ,\ j\le n\}$ is a basis of L over F.

$a_i\in L\ \ ,\ b_j\in K\Longrightarrow b_j\in L\quad\therefore a_ib_j\in L$ for all i,j

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}a_ib_j=0\quad a_{ij}\in F$$

Then

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left(a_{ij}b_j\right)a_i=0\ \ ,\sum_{j=1}^{n}a_{ij}b_j\in K$$

Since $\{a_1,\dots,a_m\}$ are linearly independent over K,

$$\sum_{j=1}^{n}a_{ij}b_j=0\ \ for\ all\ i=1,\dots,m$$

Also $\{b_1,\dots,b_n\}$ are linearly independent over F . $a_{ij}=0$ for all i=1,..,m , j=1,….1,n

$\therefore\{a_ib_j|1\le m\ ,\ 1\le j\le n\}$ is linearly independent subset of L over F.

Let $a\in L$ since $\{a_1,\dots,a_m\}$ is a basis of L over K

$$a=a_1a_1+\cdots+a_ma_m\quad ,a_i\in K$$

$a_i\in K$ and $\{b_1,\dots,b_n\}$ is a basis of K over F.

$$\Longrightarrow\beta_{i1}b_1+\cdots+\beta_{in}b_n\ \ ,\beta_{ij}\in F$$

$$a=\sum_{i=1}^{m} a_i a_i=\sum_{i=1}^{m}(\beta_{i1}b_1+\cdots+\beta_{in}b_n)\,a_i=\sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}b_jb \quad ,\beta_{ij}\in F$$

$\therefore$ $\{a_ib_j|1\le i\le m\ ,\ 1\le j\le n\}$ spans L over F and so forms a basis of L over F.

$\therefore$ $[L:F]=mn=[L:K][K:F]$

Remark :

if $[L:K]$ is finite then $[L:K]$ is also finite because $[L:K]=r\Rightarrow$every subset of L having r+1 elements is linearly dependent over F. since [L:K] is infinite , $\exists a_1,\dots,a_{r+1}\in K$ which are linearly independent over F as $1\neq 0$. As in theorem (3.4) , $a_1-1,a_2-1,\dots,a_2+1$, 1 are linearly independent over F .we fined $a_1,\dots,a_{r+1}\in L$ are linearly independent over F, a contradiction .

$\therefore$ $[L:K]$ is infinite . similarly , $[K:F]$ is infinite .

Lemma(3.5):

If f is finite extension of f, then K:F if and only if $[K:F]$ divides $[L:F]$.

Proof:

By remark above $[K:F]$ is finite as $[K:F]$ =finite also $[L:K]$ is finite . By theorem (3.4)

$$[L:K]=[L:K][K:F]$$

$[K:F]$ divides $[L:F]$

Lemma(3.6):

If k is an extension of F , then K=F if and only if $[K:F]=1$.

Proof:

If $K:F$, then $[K:F]=[K:K]=1$

If $[K:F]=1$ let {a} be a basis of K over F.

$\therefore 1\in K\Rightarrow aa\ ,a\in F\ ,a\neq 0\ \ as\ 1\neq 0\Rightarrow a=a^{-1}\in F$

Let $b\in K\Rightarrow b=\beta a\ ,\beta\in F\ \ ,\ \beta\in F\ \ ,a\in F\Rightarrow b\in F\Rightarrow K\subseteq F\ \ \Rightarrow K=F$.

Lemma(3.7):

If L is an extension of f and [L:K] is a prime number p, then there is no field K s.t $F\subset K\subset L$.

Suppose $\exists$ a field K s.t , $F\subset K\subset L$ then $p=[L:F]=[L:K][K:F]$ By theorem(3.4)

$$\Rightarrow [L:K]=1\ \ or\ [K:F]=1$$

$\Rightarrow K=L\ \ or\ K=F$ by lemma (3.7) acontradiction.

Hence the result Trivially then, if K is an extension of F of prime degree then for any $a\in K$, $F(a)=F\ \ or\ F(a)=K$

Theorem(3.8):

Let k be a finite extension of F. let [K:F]=n, let $a\in K$. Then $a,\dots,a^n$ are linearly independent over F. thus $\exists\ a_0,a_1,\dots,a_n\in F$ s.t $a_0.1+a_1a+a_na^n=0\ \ for\ some\ a_i\neq 0.$

Let $F(x) = a_0 + a_1x + a_nx^n$ $, then\ F(x)$ is non zero polynomial in f[x] as some $a_i \neq 0$, also

$$F(a) = a_0 + a_1a + a_na^n = 0$$

∴ a is algebraic over F.

∴ k is algebraic over F.

Note:

Convers of theorem (3.8) is not true.

Lemma(3.9):

$a \in K$ is algebraic over F if $[F(a): F]$ =finite

Proof:

By theorem (3.8) , F(a) is algebraic over F.

∴ $a \in F(a)$ is algebraic over F.

Converse of above lemma is also true .

Corllory 1:

If $a_1, \dots, a_n \in K$ are algebraic over F then $F(a_1, \dots, a_n)$ is finite extension of and so is algebraic over F.

Proof:

We proof the result by indication on n .if $n = 1$, result follows from cor 1. assume it to be true for naturals less than n .let $a_1, \dots, a_n \in K$ be algebraic over F. Now a_{n} is algebraic over F $\Rightarrow a_{\mathrm{n}}$ is algebraic over $F(a_1, \dots, a_n)$

By cor 1. $[F(a_1, \dots, a_{n-1})(a_{\mathrm{n}})$;$F(a_1, \dots, a_n)$ is finite by indication hypothesis,

$[F(a_1, \dots, a_n): F]$ Is finite

$[F(a_1, \dots, a_n)\ F] = [\ F(a_1, \dots, a_n): F(a_1, \dots, a_n)][F(a1, \dots .an - 1): F]$ =finite

Result is true for n also

By indication is true for all n≥ 1.

Def(3.10):

A complex number is said to be an algebraic number if it is algebraic over the field of rational numbers.

Roots of polynomials

Let F be a field and $\mathrm{f}(x) \in F[X]$.we ask whether there exists an extension K of containing a root.

Theorem(3.11):

A polynomial of degree n over a field can have at most n roots in any extension field.

Def(3.12):

Let E and L be tow extensions of a field K. An isomorphism $f: E \to L$ is called a K −isomorphism if $\mathrm{f}(a) = a$,and in that case we say E and L are K −iosmorphic. similarly we talk of K-homomorphism or K −automorphism.

Theorem(3.13):

Suppose $\sigma: K_1 \rightarrow K_2$ is an isomorphism from a field K_1 to a field K_2. Let α_1 be a zero an irreducible over polynomial $f_1(x)$ over K_1 and α_2 be zero of the corresponding polynomial $f_1(x) = \sigma(f_1(x))$ over K ,then there exists a unique isomorphism θ from $K_1(\alpha_1)$ to $K_1(\alpha_1)$ such that $\theta(\alpha_1)= \alpha_2$ and $\sigma(\alpha) = \alpha$

Proof:

Now $\varphi_1: K_1[x] \rightarrow K_2[\alpha_1]$

With $\varphi_1(g_1(x)) = g_1(\alpha_1)$

Is an onto homomorphism such that Ker $\varphi_1 = <f_1>$.

Prime subfields

Def(3.14):

Let F be a field .The intersection of all subfield of F is the smallest subfield of F and is called prime subfield of F.

Theorem(3.15):

Let P be the prime subfield of a field F. Then either $P \cong Q$ or $P \cong \frac{Z}{(P)}$,for some prime p, Z being the ring of integers.

Proof:

Define $\theta: Z \rightarrow p \subseteq F$ such that

$\theta(n) = ne$,where e denotes the unity of F

Then θ is a homomorphism.

Problem:

Show that regular pentagon is constructible.

Solution:

It would be possible to construct a pentagon if we can construct

$$\alpha = 2\cos\frac{2\pi}{5} = 2\cos 72^\circ = 2\sin 180^\circ.$$

Since $\sin 180^\circ = \frac{-1+\sqrt{5}}{4}$ which is constructible we fine it is possible to construct a regular pentagon.

Problem:

Every automorphism of a field F leaves the prime subfield P of F,element wise fixed

Solution:

Let θ be an automorphism of F

Let $K = \{a \in F | \theta(a) = a\}$

Then K is a subfield of F.

Since P is the smallest subfield of F, $P \subseteq K$ .let $b \in P$.then $b \in K$, $\Longrightarrow \theta(b) = b \Longrightarrow, \theta$ fixes element of P.

Separable Extensions

In the next we have a polynomials which have a simple roots and the field generated by these roots.

Def(3.16):

A polynomial is said to be a separable if all roots are simple.

Theorem(3.17):

A polynomial $f(x) \in F[x]$ is seperable if and only if f and f' are relatively prime.

Def(3.18):

A field K is called perfect field if every algebraic extension of K is separable.

Theorem(3.19):

Let char $K = p$. then every algebraic extension of K is seperable if and only if $K = K^P$.

Proof:

Let $a \in K$ .let $f(x) = x^{\mathrm{p}} - a$ and b be a zero of $f(x)$.then

$$0 = f(b) = b^{\mathrm{p}} - a\,, a = b^{\mathrm{p}}$$

$,f(x) = x^{\mathrm{p}} - b^{\mathrm{p}} = (x - b)^{\mathrm{p}}$.then $f(x)$ is irreducible over k.

Now α is root of $p(x)$, $\Rightarrow x - \alpha$ divides p(x) in $E[x]$

$$\Rightarrow P(x) = (x - a)q(x) \quad , \qquad q(x) \in E[X]$$

Since $deg\, p(x) = 2 \quad , deg\, q(x) = 1$.

So $q(x) = (x - \beta), \beta \in F$

Therefore $p(x) = (x - \alpha)(x - \beta)$ splits in $E[x]$.

Problem:

Let F be a perfect field .show that the set of elements fixed under all automorphisms of F is a perfect subfield.

Solution:

Let char $F = p, K = \{a \in F | \sigma(a) = a \forall \sigma \in G\}$,where G is a group of F. then K is a subfield of F.

Define $\theta: F \to F$ such that,

$$\theta(\alpha) = \alpha^{\mathrm{p}}$$

Then θ is a homomorphism, since F is perfect, θ is onto,

So $\theta \in G$, let $\alpha \in K$ .then $\sigma(\alpha) = \alpha$

$$\Rightarrow \theta(\alpha) = \alpha \Rightarrow \alpha^{\mathrm{p}} = \alpha \Rightarrow \alpha \epsilon K^{\mathrm{p}} \Rightarrow K \subseteq K^P$$

$\Rightarrow K = K^{\mathrm{p}},\ K$ is perfect.

Normal Extensions

As seen earlier if $f(x) \in K[x]$ is irreducible over K, then there extension E of K containing a root of f(x).

Def(3.20):

An extension $L: K$ is called a normal extension if every irreducible polynomial in $K[x]$ have any at least one root in L.

Theorem(3.21):

A finite normal extension is a minimal splitting field of some polynomial.

Theorem(3.22):

Let K be an algebraic closed field such that K is an extension of K.

Let $F = \{a \epsilon K | a$ is algebraic over K$\}$

Proof:

We now that$k \subseteq F \subseteq K$ is tower of field

By definition of F,F/K is algebraic

Thus F is algebraically closed

Hence F is an algebraic of K.

Lemma(3.23):

Let E be an algebraic extension of K and let $\sigma: E \rightarrow E$ be a K-homomorphism. then σ is a K-automorphism .

Proof:

Let $\alpha \in E, p(x) = Irr(K, \alpha)$,

Let $\alpha_1 = a, \alpha_1, \ldots\ldots, \alpha_r$

Let $E' = K(\alpha_1, \ldots\ldots, \alpha_r) \subseteq E$

Then E'/K is finite

Let $p(x) = (x - \alpha_{\mathrm{i}})q_{\mathrm{i}}(x)$, $q_{\mathrm{i}}(x) \in K(\alpha_{\mathrm{i}})[x]$

Since $\sigma(a) = a$ for all$a \in K$, $\sigma(p(x)) = p(x)$.

Theorem(3.24):

Let K be an algebraic extension of K, then following are equivalent.

(i) K/k is normal .

There fore $p(x) = \sigma(p(x)) = (x - \sigma(\alpha_{\mathrm{i}}))\sigma(q_{\mathrm{i}}(x))$

But $\sigma: E \rightarrow E \Longrightarrow \sigma(\alpha_{\mathrm{i}}) \in E$ for all i

So $\sigma(\alpha_{\mathrm{i}}) \in E'$ for all i,

$\Longrightarrow \sigma: E \rightarrow E'$ is a K-homomorphism

Also E'/K is finite

Since σ is also 1-1

So $\sigma: E' \rightarrow E'$ IS on to, σ is a K-automorphism of E.

Galois Extensions

Def(3.25):

An extension E of F is called a Galois extension if E/F is finite .f is the fixed of a group of automorphisms of E.

Theorem(3.26):

Let E/F be a finite extension .then E/F is a Galois extension if and only if it is both normal and seperable.

Note:

When E/F is Galois, the group of all F-automorphisms of E is denoted by $Gal(E/F)$ or $G(E/F)$ called the Galois group of E/F.

Corllory 2:

Let char $K = 0$.then K is contained in some Galois extension of K.

Proof:

Let f(x) be a non constant polynomial in $K[x]$.Let E be a minimal splitting field of f(x) over K .then E/K is finite normal .Since is perfect, ⟹E/K is seperable ,

So, E/K is Galois.

Theorem (3.27):

Let E/F be a finite extension .then E/F is contained in Galois extension if and only if it is seperable.

Proof:

Let E/F be contained in Galois extension E'/F.then $F \subseteq E \subseteq E'$

Now E'/F is Galois $\Longrightarrow$ E'/F is seperable E/F' is seperable

Conversely, Let E/F be seperable. since E/F is finite,$E = F(a_1, \dots, a_n)$

Let $p_i = Irr(F, \alpha_i)$, $\alpha_i \in E$. $\alpha_i \in E \Longrightarrow \alpha_i$ is seperable over F$\Longrightarrow \alpha_i$ is a simple zero of p_i ⟹each zero of p_i in a splitting field is simple.

Reference

(1) A First course in ABSTRACT ALGEBRA. Johb. Fraleigh
Department of Mathematics, university of Rhode Island.
Copyright 1982,1976,1967, by Addison-wesley publishing company.Inc
(2) BELL, ERIGT. Men of Mathematics. NewYork: Simon and Schuster, 1986.
(3) BURTON, DAVID M. The History of Mathematics, 4th ed.
New York:Mc Graw Hill, 1998.