Semester – V

17MMU501A	RING THEORY AND LINEAR ALGEBRA I	L T P C
		6 2 0 6

Scope: On successful completion of course the learners gain about the linear transformations, homomorphism, isomorphism and its properties.

Objectives: To enable the students to learn and gain knowledge about rings, subrings, vector spaces, subspaces, algebra of subspaces, isomorphism and its properties.

UNIT I
RINGS
Definition and examples of rings - Properties of rings - Subrings - Integral domains and fields - Characteristic of a ring. Ideal - Ideal generated by a subset of a ring - Factor rings - Operations on ideals - Prime and maximal ideals.

UNIT II
RING HOMOMORPHISMS
Ring homomorphisms - Properties of ring homomorphisms - Isomorphism theorems I, II and III - Field of quotients.

UNIT III
VECTOR SPACES
Vector spaces - Subspaces - Algebra of subspaces - Quotient spaces - Linear combination of vectors - Linear span - Linear independence - Basis and dimension - Dimension of subspaces.

UNIT IV
LINEAR TRANSFORMATIONS
Linear transformations - Null space - Range - Rank and nullity of a linear transformation – Matrix representation of a linear transformation - Algebra of linear transformations.

UNIT V
ISOMORPHISM
Isomorphism theorems -Invertability and isomorphisms - change of coordinate matrix.

SUGGESTED READINGS

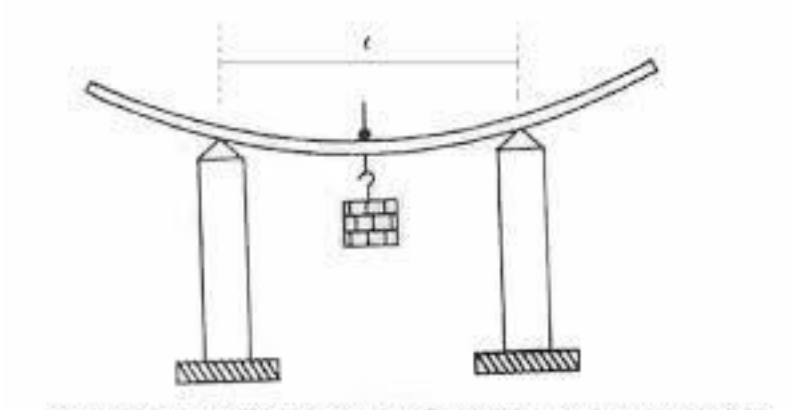
TEXT BOOK

1. Fraleigh.J.B., (2004). A First Course in Abstract Algebra , Seventh Edition , Pearson Education Ltd, Singapore.

REFERENCES
1. Joseph A. Gallian., (2013). Contemporary Abstract Algebra, Fourth Edition, Narosa Publishing House, New Delhi.

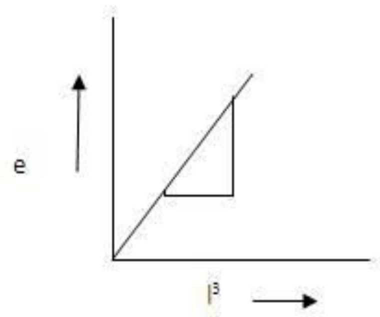
2. Kumaresan S., (2000). Linear Algebra- A Geometric Approach, Prentice Hall of India, New Delhi.

DIAGRAM



YOUNG'S MODULUS - NON-UNIFORM BENDING

Graph between depression and length



1. YOUNG'S MODULUS – NON UNIFORM BENDING PIN AND MICROSCOPE

Expt No:01

AIM

To find the Young's modulus of the given material bar by non uniform bending using pin and microscope method.

APPARATUS

Pin and Microscope arrangement, Scale ,Vernier calipers, Screw gauge, Weight hanger, Material bar or rod.

THEORY

Young's modulus is named after Thomas Young,19th century ,British scientist. In solid mechanics, Young's modulus is defines as the ratio of the longitudinal stress over longitudinal strain, in the range of elasticity the Hook's law holds (stress is directly proportional to strain). It is a measure of stiffness of elastic material.

If a wire of length L and area of cross-section 'a' be stretched by a force F and if a change (increase) of length 'l' is produced, then

$$Young's\ modulus = \frac{Normal\ stress}{Longitudinal\ strain} = \frac{F/a}{l/L}$$

Non Uniform Bending Using Pin and Microscope

Here the given beam(meter scale) is supoorted symmetrically on two knife edges and loaded at its centre. The maximum depression is produced at its centre. Since the load is applied only one point of the beam, the bending is not uniform through out the beam and the bending of the beam is called non- uniform bending.

In non-uniform bending (central loading), the Young's modulus of the material of the bar is given by

$$Y = \frac{mgl^3}{48Ie}$$

I is the moment of inertia of the bar.

For a rectangular bar**,**

$$I = \frac{bd^3}{12}$$

Substituting (4) in (3)

In non uniform bending, the young's modulus of the material of the bar is given by,

OBSERVATIONS

Value of 1 M.S.D = 1/20
Number of divisions on the vernier, n = 50
Least count of microscope = 1 m.s.d/n = 1/1000 = 0.001 cm

No	Distance of the knife edges , l (cm)	Load M(kg)	Telescope reading			depression for load 4m, e (cm)	Mean e (cm)	$\frac{l^3}{e}$ (cm^3)	Mean $\frac{l^3}{e}$ (cm^3)
			Loading (cm)	unloading (cm)	mean (cm)				
1		Wo Wo+m Wo+2m Wo+3m Wo+4m Wo+5m Wo+6m Wo+7m			Xo X1 X2 X3 X4 X5 X6 X7	X4-X0 X5-X1 X6-X2 X7-X3			
2									
3									
4									

CALCULATIONS

Thickness of the material bar "d" = ……………………….. mm.
Breadth of the material bar "b" = ……………………………cm.
Mean value of l^3/e = ………………………….m.
Load applied for depression "e" = ………………………… m.

Young's modulus of the material bar , $Y = \frac{mgl^3}{4bd^3e}$ = …………………………N/m^2.

$$Y = \frac{mgl^3}{4bd^3e}$$

m - Mass loaded for depression.

g - Acceleration due to gravity.

l - Length between knife edges.

b - Breadth of the bar using vernier calipers.

d - Thickness of the bar using screw gauge.

e - Depression of the bar.

PROCEDURE

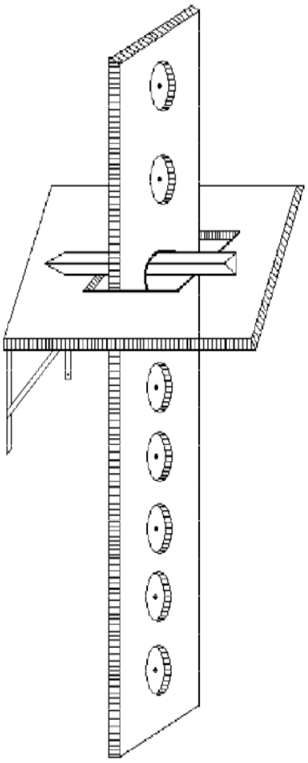
1. Select the environment and material for doing experiment.
2. Choose mass, length , breadth and thickness of the material bar using sliders on the right side of the simulator .
3. Fix the distance between knife edges.
4. Focussing the microscope and adjusting the tip of the pin coincides with the point of intersection of the cross wires using left and top knobs on microscope respectively.
5. Readings are noted using the microscope reading for 0g. Zoomed part of microscope scale is available by clicking the centre part of the apparatus in the simulator. Total reading of microsope is MSR+VSR*LC. MSR is the value of main scale reading of the microsope which is coinciding exacle with the zero of vernier scale. One of the division in the vernier scale coincides exactly with the main scale is the value of VSR. LC is the least count.
6. Weights are added one by one say 50g, then pin moves downwards while viewing through microscope. Again adjust the pin such that it coincides exactly with the cross wire.
7. The readings are tabulated and Y is determined using equation (2).

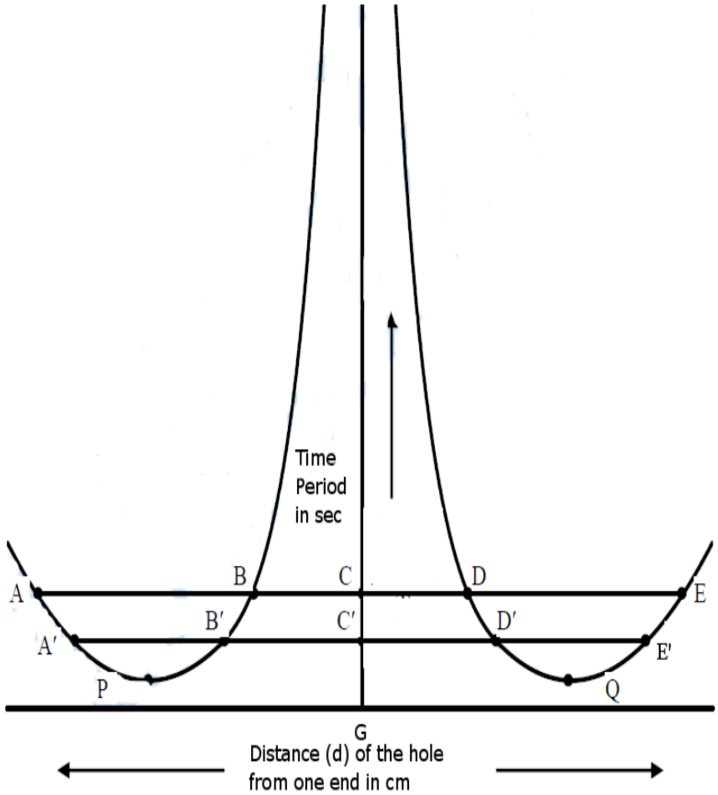
From graph $\frac{l^3}{e}$ can be calculated.

RESULT

Young's modulus of the given material using non uniform bending method =..................................Nm^{-2}.

DIAGRAM





OBSERVATIONS:

To draw graph :

No.of holes from A	Distance of knife edge from A: (cm)	Time for 10 oscillations (s)			Time period T (s)
		1	2	Mean (s)	

2. MEASUREMENT OF ACCELERATION DUE TO GRAVITY (G) BY A COMPOUND PENDULUM

Expt No 02

AIM

To determine the acceleration due to gravity (g) by means of a compound pendulum.

APPARATUS

(i) A bar pendulum, (ii) a knife–edge with a platform, (iii) a sprit level, (iv) a precision stop watch, (v) a meter scale and (vi) a telescope.

FORMULA

Acceleration of gravity, $g= 4\pi^2(2k_G/T_{min}^2)$

PROCEDURE

(i) Suspend the bar using the knife edge of the hook through a hole nearest to one end of the bar. With the bar at rest, focus a telescope so that the vertical cross-wire of the telescope is coincident with the vertical mark on the bar.

(ii) Allow the bar to oscillate in a vertical plane with small amplitude (within 4^0 of arc).

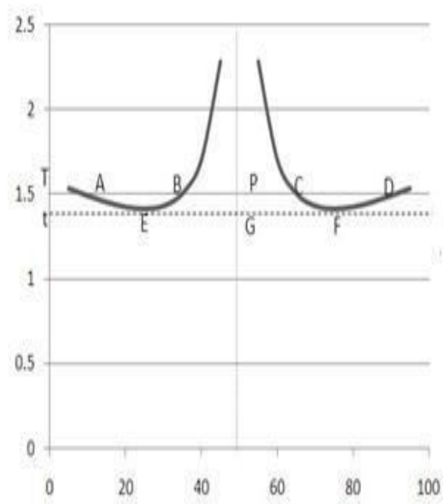
(iii) Note the time for 20 oscillations by a precision stop-watch by observing the transits of the vertical line on the bar through the telescope. Make this observation three times and find the mean time t for 20 oscillations. Determine the time period T.

(iv) Measure the distance d of the axis of the suspension, i.e. the hole from one of the edges of the bar by a meter scale.

(v) Repeat operation (i) to (iv) for the other holes till C.G of the bar is approached where the time period becomes very large.

To find the value of 'g' :

SI.No	Length of equivalent simple pendulum(cm)			Time period, T (s)	g (cm/s^2)
	AC (cm)	BD (cm)	Mean l		



CALCULATION

To find the radius of gyration and the acceleration of gravity (step 3 above):

Radius of gyration about the centre of mass k_G = EF/2 = ...
.
Acceleration of gravity, g= $4\pi^2(2k_G/T_{min}^2)$ = ...

To find the radius of gyration (step 4 above):

SI.No	h=AD/2	h' =BC/2	$k_G=(hh')^{1/2}$

RESULTS:

Average acceleration of gravity, $g= 4\pi^2(l/T^2)$ = ... m/s^2

1) Average radius of gyration of the pendulum about its centre of mass, k_G = ... m
2) Mass of the pendulum M = ... Kg
3) Moment of inertia of the pendulum about its centre of mass, $I_G=Mk_G^2$ = ... Kgm^2

DIAGRAM

Fig.6.4 Spectrometer – Angle of Prism

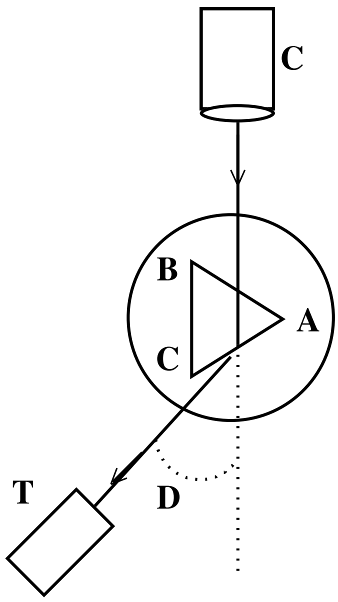
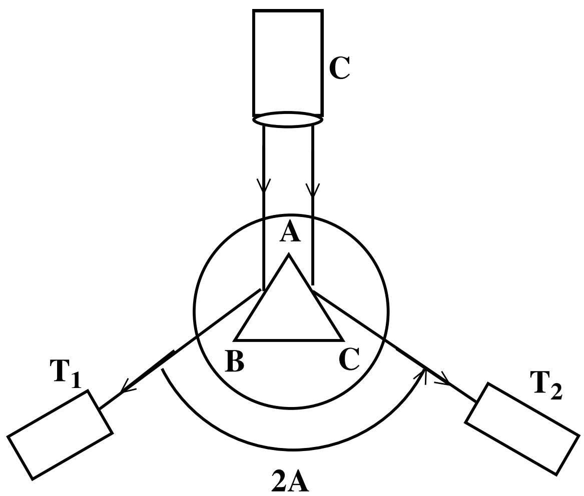


Fig.6.5 Angle of Minimum Deviation



3. DETERMINATION OF DISPERSIVE POWER OF A PRISM USING SPECTROMETER

Expt No.03

AIM

To determine the dispersive power of a given prism for any two prominent lines of the mercury spectrum.

APPARATUS

A spectrometer, mercury vapour lamp, prism, spirit level, reading lens etc.

FORMULAE

1. Refractive index of the prism for any particular colour

$$\mu = \frac{\sin\left(\frac{A+D}{2}\right)}{\sin\left[\frac{A}{2}\right]}$$

where A = Angle of the prism in (deg)

D = Angle of minimum deviation for each colour in (deg)

2. The dispersive power of the prism is

$$\omega = \frac{\mu_1 - \mu_2}{\left(\frac{\mu_1 + \mu_2}{2}\right) - 1}$$

where μ_1 and μ_2 are the refractive indices of the given prism for any two colours.

PROCEDURE

Part I : To determine the angle of the prism (A)

1. The initial adjustments of the spectrometer like, adjustment of the telescope for the distant object, adjustment of eye piece for distinct vision of cross –wires, levelling the prism table using spirit level, and adjustment of collimator for parallel rays are made as usual.
2. Now the slit of the collimator is illuminated by the mercury vapour lamp.
3. The given prism is mounted vertically at the centre of the prism table, with its refracting edge facing the collimator as shown in figure (6.4) (i.e.) the base of the prism must face the telescope. Now the parallel ray of light emerging from the collimator is incident on both the refracting surfaces of the prism.
4. The telescope is released and rotated to catch the image of the slit as reflected by one refracting face of the prism.

OBSERVATIONS

$$LC = \frac{\text{Value of one MSD}}{\text{No. of div on VS}} = \frac{30'}{30} = 1'$$

Table 6.7: To determine the angle of prism (A)

LC = 1’ TR = MSR + (VSC ×LC)

Position of the reflected ray	Vernier –A			Vernier-B		
	MSR degree	VSC div	T.R degree	MSR degree	VSC div	T.R degree
Left side			(R_1)			(R_3)
Right Side			(R_2)			(R_4)
	$2A = (R_1 - R_2) =$ $\therefore A = \frac{R_1 - R_2}{2}$ A=			$2A = (R_3 - R_4) =$ $\therefore A = \frac{R_3 - R_4}{2}$ $\therefore$ A=		

$\therefore$ Mean A =

5. The telescope is fixed with the help of main screw and the tangential screw is adjusted until the vertical cross-wire coincides with the fixed edge of the image of the slit. The main scale and vernier scale readings are taken for both the verniers.
6. Similarly the readings corresponding to the reflected image of the slit on the other face are also taken. The difference between the two sets of the readings gives twice the angle of the prism (2A). Hence the angle of the prism A is determined.

Part 2 : To determine the angle of the minimum deviation (D) and Dispersive power of the material of the prism

1. The prism table is turned such that the beam of light from the collimator is incident on one polished face of the prism and emerges out from the other refracting face. The refracted rays (constituting a line spectrum) are received in the telescope Fig. 6.5.
2. Looking through the telescope the prism table is rotated such that the entire spectrum moves towards the direct ray, and at one particular position it retraces its path. This position is the minimum deviation position.
3. Minimum deviation of one particular line, say violet line is obtained. The readings of both the verniers are taken.
4. In this manner, the prism must be independently set for minimum deviation of red line of the spectrum and readings of the both the verniers are taken.
5. Next the prism is removed and the direct reading of the slit is taken.
6. The difference between the direct reading and the refracted ray reading corresponding to the minimum deviation of violet and red colours gives the angle of minimum deviation (D) of the two colours.
7. Thus, the refractive index for each colour is calculated, using the general formula.

$$\mu = \frac{\sin \frac{(A+D)}{2}}{\sin A/2}$$

and Dispersive power of the prism.

$$\omega = \frac{\mu_1 - \mu_2}{\left(\frac{\mu_1 + \mu_2}{2}\right) - 1}$$

To determine the angle of the minimum deviation (D) and Dispersive power of the material of the prism:

Direct ray reading (R_1) : Vernier A : Vernier B:

LC = 1’ TR = MSR + (VSC ×LC)

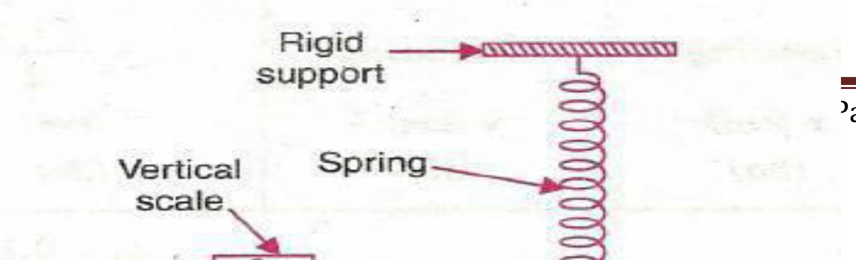
<table>
<tr><th rowspan="3">Line</th><th colspan="6">Refracted ray readings when the prism is in minimum deviation position(R_2)</th><th colspan="2">Angle of minimum deviation (D) (= $R_1 \sim R_2$)</th><th rowspan="3">Mean D</th></tr>
<tr><th colspan="3">Vernier –A</th><th colspan="3">Vernier -B</th><th rowspan="2">Vernier –A degree</th><th rowspan="2">Vernier-B degree</th></tr>
<tr><th>MSR degree</th><th>VSC div</th><th>TR degree</th><th>MSR Degree</th><th>VSC div</th><th>T.R degree</th></tr>
<tr><td>Violet</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Red</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Mean (D) :

Result

The dispersive power of the material of the prism is -------------

DIAGRAM



OBSERVATION

Least count of vertical scale = 0.1 cm.

Table for load and extension

Serial No.	Load (g)	Reading of the scale while		Extension x (cm)
		Loading	Unloading	
1				
2				
3				
4				
5				

4. DETERMINATION OF SPRING CONSTANT OF THE GIVEN SPRING

Expt No:04

AIM

To find the force constant of a helical spring by plotting graph between load and extension.

APPARATUS

Spring, a rigid support, slotted weights, a vertical wooden scale, a fine pointer, a hook.

THEORY

When a load *F* suspended from lower free end of a spring hanging from a rigid support, it increases its length by amount *x*,

then $F \ a \ x$

or $F = k\,x$,

where *k* is constant of proportionality.
It is called the force constant or the spring constant of the spring.

PROCEDURE

1. Suspend the spring from a rigid support. Attach a pointer and a hook from . free end.
2. Hang a 20 g hanger from the hook.
3. Set the vertical wooden scale such that the tip of the pointer comes over the scale.
4. Note the reading of the position of the tip of the pointer on the scale. Record the reading in loading column against zero load. .

CALCULATIONS

From graph,

k =……………… gwt per cm.

Gently add a 20 g slotted weight to the hanger. The pointer tip moves down. Wait for few minutes till the pointer tip comes to rest. Repeat step 4.

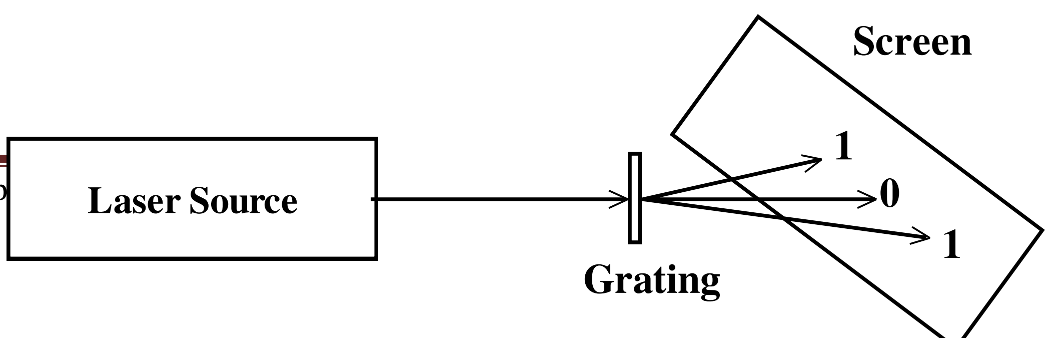
6. Repeat steps 5 and 6 till five slotted weights have been added.
7. Now remove one slotted weight. The pointer tip moves up. Repeat step 6. Record the reading in unloading column.

8. Repeat step 8 till only hanger is left.
Record your observations as given below.

RESULT

The force constant of the given spring is …………. g wt per cm.

DIAGRAM



Experimental Setup for Laser Grating

5. DETERMINATION OF LASER PARAMETERS – DIVERGENCE AND WAVELENGTH FOR A GIVEN LASER SOURCE USING LASER GRATING

Expt No:05

AIM

To determine the divergence and wavelength of the given laser source using standard grating.

APPARATUS

Laser source, grating, a screen etc.,

PRINCIPLE

When a composite beam of laser light is incident normally on a plane diffraction grating, the different components are diffracted in different directions. The m^{th} order maxima of the wavelength λ, will be formed in a direction θ if d sin θ = mλ, where d is the distance between two lines in the grating.

FORMULA

1. The angle of divergence is given by

$$\Phi = \frac{(a_2 - a_1)}{2(d_2 - d_1)}$$

where a_1 = Diameter of the laser spot at distance d_1 from the laser source

a_2 = Diameter of the laser spot at distance d_2 from the laser source

2. The wavelength of the laser light is given by

$$\lambda = \frac{\sin\theta_m}{Nm} \quad \text{m}$$

where m = Order of diffraction

θ_n = Angle of diffraction corresponding to the order m

N = number of lines per metre length of the grating

θ = $\tan^{-1}$ (x/D)

x = Distance from the central spot to the diffracted spot (m)

D = Distance between grating and screen(m)

OBSERVATION

Determination of wave length of Laser Light:

Distance between grating and screen (D) = ----------- m

Number of lines per metre length of the grating = N = --------------

S.No	Order of Diffraction (m)	Distance of Different orders from the Central Spot (x) m	Mean (x) m	Angle of diffraction θ = $\tan^{-1}[x$ /	$\lambda = \frac{\sin\theta_m}{Nm}$

		Left	Right		D]	Å

CALCULATION

The angle of divergence

a_1 = Diameter of the laser spot at distance d_1 from the laser source =
a_2 = Diameter of the laser spot at distance d_2 from the laser source =

$$\Phi = \frac{(a_2 - a_1)}{2(d_2 - d_1)}$$

The wavelength of the laser light

m = Order of diffraction =

θ_n = Angle of diffraction corresponding to the order m =

N = number of lines per metre length of the grating =

θ = $\tan^{-1}$ (x/D) =

x = Distance from the central spot to the diffracted spot (m) =

D = Distance between grating and screen(m) =

$$\lambda = \frac{\sin\theta_m}{Nm} \quad \text{m}$$

PROCEDURE

Part 1: Determination of angle of divergence

1. Laser source is kept horizontally.
2. A screen is placed at a distance d_1 from the source and the diameter of the spot (a_1) is measured.
3. The screen is moved to a distance d_2 from the source and at this distance, the diameter of the spot (a_2) is measured.

Part 2: Determination of wavelength

1. A plane transmission grating is placed normal to the laser beam.
2. This is done by adjusting the grating in such a way that the reflected laser beam coincides with beam coming out of the laser source.
3. The laser is switched on. The source is exposed to grating and it is diffracted by it.
4. The other sides of the grating on the screen, the diffracted images (spots) are seen.
5. The distances of different orders from the central spot are measured.
6. The distance from the grating to the screen (D) is measured.
7. θ is calculated by the formula $\theta = \tan^{-1}(x/d)$.
8. Substituting the value of θ, N and m in the above formula, the wavelength of the given monochromatic beam can be calculated.

RESULT

1. The angle of divergence is = -----------.
2. The wavelength of the given monochromatic source is = ----------- Å

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University Established Under Section 3 of UGC Act 1956)

Coimbatore – 641 021.

LECTURE PLAN
DEPARTMENT OF MATHEMATICS

Staff name: U.R.Ramakrishnan
Subject Name: Ring Theory and Linear Algebra I **Sub.Code:17MMU501A**
Semester: V **Class: III B. Sc Mathematics**

S.No	Lecture Duration Period	Topics to be Covered	Support Material/ Page Nos
		UNIT-I	
1.	1	Definition and examples of rings	R1: Ch 12, 237-239
2.	1	Continuation of examples on rings	R1: Ch 12, 237-239
3.	1	Properties of rings	R1: Ch 12, 239-240
4.	1	Tutorial-1	
5.	1	Theorems on sub rings	R1: Ch 12, 241-242
6.	1	Integral domains	R1: Ch 13, 249-250
7.	1	Theorems on fields	R1: Ch 13, 250-251
8.	1	Tutorial-2	
9.	1	Characteristic of a ring	R1: Ch 13, 251-252
10.	1	Theorems on ideal	R1: Ch 13, 252-253
11.	1	Theorems on ideal generated by a subset of a ring	R1: Ch 13, 253-254
12.	1	Tutorial-3	
13.	1	Definition and examples on factor ring	R1: Ch 13, 254-245
14.	1	Theorems on factor rings	R1: Ch 14, 262-263
15.	1	Operations on ideals	R1: Ch 14, 262-263
16.	1	Tutorial-4	
17.	1	Theorems on prime ideals	R1: Ch 14, 264-266

18.	1	Theorems on maximal ideals	R1: Ch 14, 264-266
19.	1	Problems on maximal ideals	R1: Ch 14, 267-268
20.	1	Tutorial-5	R1: Ch 14, 268-269
21.	1	Recapitulation and Discussion of possible questions	
	Total No of Hours Planned For Unit 1=21		
1.	1	Definitions and examples on ring homomorphisms	R1: Ch 15, 280-281
2.	1	Theorems on ring homomorphisms	R1: Ch 15, 281-282
3.	1	Tutorial-1	
4.	1	Continuation of theorems on ring homomorphisms	R1: Ch 15, 282-283
5.	1	properties of ring homomorphisms	R1: Ch 15, 283-284
6.	1	Continuation of properties on ring homomorphisms	R1: Ch 15, 284-285
7.	1	Tutorial-2	
8.	1	Continuation of properties on ring homomorphisms	R1: Ch 15, 285
9.	1	Continuation of properties on ring homomorphisms	R1: Ch 15, 285-286
10.	1	Isomorphism theorem I	T1: Ch 7, 301-302
11.	1	Tutorial-3	
12.	1	Isomorphism theorem II	T1: Ch 7, 303-305
13.	1	Continuation of isomorphism theorem II	T1: Ch 7, 303-305
14.	1	Isomorphism theorem III	T1: Ch 7, 306-309
15.	1	Tutorial-4	
16.	1	Continuation of isomorphism theorem III	T1: Ch 7, 306-309
17.	1	Theorems on field of quotients	T1: Ch 7, 309-310
18.	1	Theorems on field of quotients	T1: Ch 7, 310-311

19.	1	Tutorial-5	
20.	1	Recapitulation and Discussion of possible questions	
	Total No of Hours Planned For Unit II=20		
		UNIT-III	
1.	1	Introduction to Vector spaces	R1: Ch 19, 345-346
2.	1	Theorems on subspaces	R1: Ch 19, 346-347
3.	1	Tutorial-1	
4.	1	Continuation of theorems on subspaces	R1: Ch 19, 347-348
5.	1	Theorems on spaces	R1: Ch 19, 348-349
6.	1	properties of subspaces	T1: Ch 6, 283-284
7.	1	Tutorial-2	
8.	1	Theorems on algebra of subspaces	T1: Ch 6, 285-286
9.	1	Theorems on quotient spaces	T1: Ch 6, 287-288
10.	1	Theorems on linear span	T1: Ch 6, 289-290
11.	1	Tutorial-3	
12.	1	Theorems on linear independence	T1: Ch 6, 291-292
13.	1	Theorems on basis and dimension	T1: Ch 6, 293-294
14.	1	Theorems on dimension of subspaces	
15.	1	Tutorial-4	T1: Ch 6, 294
16.	1	Theorems on dimension of subspaces	T1: Ch 6, 295-296
17.	1	Recapitulation and Discussion of possible questions	
	Total No of Hours Planned For Unit III=17		
		UNIT-IV	
1.	1	Linear transformations-Definition and examples	T: Ch 2, 33

2.	1	Tutorial-1	
3.	1	Theorems on linear transformations	R1: Ch 9, 212-213
4.	1	Theorems on null space	R1: Ch 9, 214-215
5.	1	Continuation of theorems on null space	R1: Ch 9, 217-219
6.	1	Tutorial-2	
7.	1	properties of null space	R1: Ch 9, 220-223
8.	1	Theorems on range	R2: Ch 11, 320-323
9.	1	Theorems on rank of a linear transformation	R2: Ch 11, 324-325
10.	1	Tutorial-3	
11.	1	Theorems on nullity of a linear transformation	R2: Ch 11, 326-327
12.	1	Theorems on matrix representation of a linear transformation	R2: Ch 11, 327-329
13.	1	Continuation of theorems on matrix representation of a linear transformation	R2: Ch 11, 330-332
14.	1	Tutorial-4	
15.	1	Theorems on algebra of linear transformations	R2: Ch 11, 333-334
16.	1	Continuation of theorems on algebra of linear transformations	R2: Ch 11, 335-337
17.	1	Continuation of theorems on algebra of linear transformations	
18.	1	Tutorial-5	
19.	1	Recapitulation and Disscussion of possible questions	
	Total No of Hours Planned For Unit IV=19		
		UNIT-V	
1.	1	Isomorphism theorems	R2: Ch 12, 340-343
2.	1	Isomorphism theorems	R2: Ch 12, 344-345
3.		Tutorial-1	

4.	1	Isomorphism theorems	R2: Ch 12, 346-347
5.	1	Isomorphism theorems	R2: Ch 12, 348-349
6.	1	Theorems on invertibility and isomorphisms	R2: Ch 12, 350-353
7.		Tutorial-2	
8.	1	Theorems on invertibility and isomorphisms	R2: Ch 12, 354-355
9.	1	Theorems on invertibility and isomorphisms	R2: Ch 12, 356-357
10.	1	Theorems on change of coordinate matrix	R2: Ch 12, 358-359
11.		Tutorial-3	
12.	1	Theorems on change of coordinate matrix	R2: Ch 12, 360-361
13.	1	Theorems on change of coordinate matrix n	R2: Ch 12, 362-363
14.	1	Theorems on change of coordinate matrix n	R2: Ch 12, 362-363
15.	1	Tutorial-4	
16.	1	Recapitulation and Discussion of possible questions	
17.	1	Discussion of previous year ESE questions	
18.	1	Discussion of previous year ESE questions	
19.	1	Discussion of previous year ESE questions	
	Total No of Hours Planned for unit V=19		
	Total Planned Hours-96		

SUGGESTED READINGS

TEXT BOOK

1. David M. Burton, (2007). Elementary Number Theory, Sixth Edition, Tata McGraw-Hill, Delhi.

REFERENCES

1. Neville Robinns, (2007). Beginning Number Theory, 2nd Ed., Narosa Publishing House Pvt. Ltd., Delhi.
2. Neal Koblitz., (2006).A course in Number theory and cryptography,Second Edition, Hindustan Book Agency, New Delhi.

UNIT-I

SYLLABUS

RINGS

Definition and examples of rings - Properties of rings - Subrings - Integral domains and fields - Characteristic of a ring. Ideal - Ideal generated by a subset of a ring - Factor rings - Operations on ideals - Prime and maximal ideals.

RINGS

Definition Ring

A *ring* R is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all a, b, c in R:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. **There is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all a in R.**
4. **There is an element $-a$ in R such that $a + (-a) = 0$.**
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ **and** $(b + c)a = ba + ca$.

So, a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition. Note that multiplication need not be commutative. When it is, we say that the ring is *commutative*. Also, a ring need not have an identity under multiplication. A *unity* (or *identity*) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a *unit* of the ring. Thus, a is a unit if a^{-1} exists.

The following terminology and notation are convenient. If a and b belong to a commutative ring R and a is nonzero, we say that *a divides b* (or that a is a *factor* of b) and write $a \mid b$, if there exists an element c in R such that $b = ac$. If a does not divide b, we write $a \nmid b$.

Recall that if a is an element from a group under the operation of addition and n is a positive integer, na means $a + a + \cdots + a$, where there are n summands. When dealing with rings, this notation can cause confusion, since we also use juxtaposition for the ring multiplication. When there is the potential for confusion, we will use $n \cdot a$ to mean $a + a + \cdots + a$ (n summands).

Examples of Ring

EXAMPLE 1 The set Z of integers under ordinary addition and multiplication is a commutative ring with unity 1. The units of Z are 1 and -1. ∎

EXAMPLE 2 The set $Z_n = \{0, 1, \ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring with unity 1. The set of units is $U(n)$. ∎

EXAMPLE 3 The set $Z[x]$ of all polynomials in the variable x with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$. ∎

EXAMPLE 4 The set $M_2(Z)$ of 2×2 matrices with integer entries is a noncommutative ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. ∎

EXAMPLE 5 The set $2Z$ of even integers under ordinary addition and multiplication is a commutative ring without unity. ∎

EXAMPLE 6 The set of all continuous real-valued functions of a real variable whose graphs pass through the point $(1, 0)$ is a commutative ring without unity under the operations of pointwise addition and multiplication [that is, the operations $(f + g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$]. ∎

EXAMPLE 7 Let $R_1, R_2, \ldots, R_n$ be rings. We can use these to construct a new ring as follows. Let

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}$$

and perform componentwise addition and multiplication; that is, define

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

and

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

This ring is called the *direct sum* of $R_1, R_2, \ldots, R_n$. ∎

Properties of Rings:

Theorem

Let a, b, and c belong to a ring R. Then

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.[†]
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore, if R has a unity element 1, then

5. $(-1)a = -a$.
6. $(-1)(-1) = 1$.

PROOF We will prove rules 1 and 2 and leave the rest as easy exercises (see Exercise 11). To prove statements such as those in Theorem 12.1, we need only "play off" the distributive property against the fact that R is a group under addition with additive identity 0. Consider rule 1. Clearly,

$$0 + a0 = a0 = a(0 + 0) = a0 + a0.$$

So, by cancellation, $0 = a0$. Similarly, $0a = 0$.

To prove rule 2, we observe that $a(-b) + ab = a(-b + b) = a0 = 0$. So, adding $-(ab)$ to both sides yields $a(-b) = -(ab)$. The remainder of rule 2 is done analogously. ∎

Theorem

If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Many students have the mistaken tendency to treat a ring as if it were a group under *multiplication*. It is not. The two most common errors are the assumptions that ring elements have multiplicative inverses—they need not—and that a ring has a multiplicative identity—it need not. For example, if a, b, and c belong to a ring, $a \neq 0$ and $ab = ac$, we *cannot* conclude that $b = c$. Similarly, if $a^2 = a$, we *cannot* conclude that $a = 0$ or 1 (as is the case with real numbers). In the first place, the ring need not have multiplicative cancellation, and in the second place, the ring need not have a multiplicative identity. There is an important class of rings that contains Z and $Z[x]$ wherein multiplicative identities exist and for which multiplicative cancellation holds. This class is taken up in the next chapter.

Subrings:

Definition Subring

A subset S of a ring R is a *subring of* R if S is itself a ring with the operations of R.

Theorem

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication—that is, if $a - b$ and ab are in S whenever a and b are in S.

PROOF Since addition in R is commutative and S is closed under subtraction, we know by the One-Step Subgroup Test (Theorem 3.1) that S is an Abelian group under addition. Also, since multiplication in R is associative as well as distributive over addition, the same is true for multiplication in S. Thus, the only condition remaining to be checked is that multiplication is a binary operation on S. But this is exactly what closure means. ■

■ **EXAMPLE 8** $\{0\}$ and R are subrings of any ring R. $\{0\}$ is called the *trivial* subring of R. ■

■ **EXAMPLE 9** $\{0, 2, 4\}$ is a subring of the ring Z_6, the integers modulo 6. Note that although 1 is the unity in Z_6, 4 is the unity in $\{0, 2, 4\}$. ■

■ **EXAMPLE 10** For each positive integer n, the set

$$nZ = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$$

is a subring of the integers Z. ■

■ **EXAMPLE 11** The set of Gaussian integers

$$Z[i] = \{a + bi \mid a, b \in Z\}$$

is a subring of the complex numbers **C.** ■

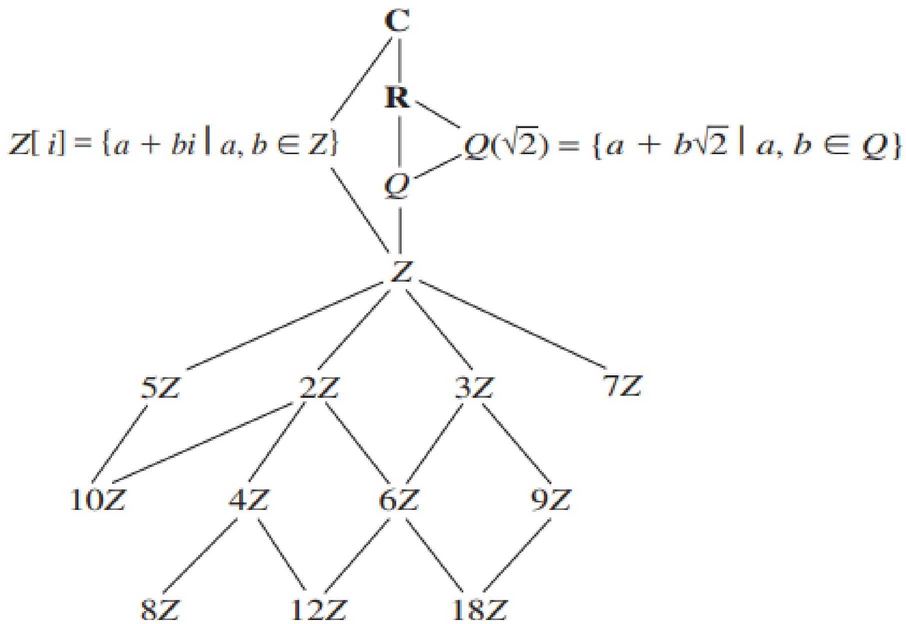
■ **EXAMPLE 12** Let R be the ring of all real-valued functions of a single real variable under pointwise addition and multiplication. The subset S of R of functions whose graphs pass through the origin forms a subring of R. ■

■ **EXAMPLE 13** The set

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

of diagonal matrices is a subring of the ring of all 2×2 matrices over Z. ■

We can picture the relationship between a ring and its various subrings by way of a subring lattice diagram. In such a diagram, any ring is a subring of all the rings that it is connected to by one or more upward lines. Figure 12.1 shows the relationships among some of the rings we have already discussed.



In the next several chapters, we will see that many of the fundamental concepts of group theory can be naturally extended to rings. In particular, we will introduce ring homomorphisms and factor rings.

Integral Domain:

Definition Zero-Divisors

A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition Integral Domain

An *integral domain* is a commutative ring with unity and no zero-divisors.

Thus, in an integral domain, a product is 0 only when one of the factors is 0; that is, $ab = 0$ only when $a = 0$ or $b = 0$. The following examples show that many familiar rings are integral domains and some familiar rings are not. For each example, the student should verify the assertion made.

EXAMPLE 1 The ring of integers is an integral domain. ■

■ **EXAMPLE 2** The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is an integral domain. ■

■ **EXAMPLE 3** The ring $Z[x]$ of polynomials with integer coefficients is an integral domain. ■

■ **EXAMPLE 4** The ring $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ is an integral domain. ■

■ **EXAMPLE 5** The ring Z_p of integers modulo a prime p is an integral domain. ■

■ **EXAMPLE 6** The ring Z_n of integers modulo n is *not* an integral domain when n is not prime. ■

■ **EXAMPLE 7** The ring $M_2(Z)$ of 2×2 matrices over the integers is *not* an integral domain. ■

■ **EXAMPLE 8** $Z \oplus Z$ is *not* an integral domain. ■

What makes integral domains particularly appealing is that they have an important multiplicative group theoretic property, in spite of the fact that the nonzero elements need not form a group under multiplication. This property is cancellation.

Theorem

Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

PROOF From $ab = ac$, we have $a(b - c) = 0$. Since $a \neq 0$, we must have $b - c = 0$. ■

Field:

Definition Field

A *field* is a commutative ring with unity in which every nonzero element is a unit.

To verify that every field is an integral domain, observe that if a and b belong to a field with $a \neq 0$ and $ab = 0$, we can multiply both sides of the last expression by a^{-1} to obtain $b = 0$.

It is often helpful to think of ab^{-1} as a divided by b. With this in mind, a field can be thought of as simply an algebraic system that is closed under addition, subtraction, multiplication, and division (except by 0). We have had numerous examples of fields: the complex numbers, the real numbers, the rational numbers. The abstract theory of fields was initiated by Heinrich Weber in 1893. Groups, rings, and fields are the three main branches of abstract algebra. Theorem 13.2 says that, in the finite case, fields and integral domains are the same.

Theorem

A finite integral domain is a field.

PROOF Let D be a finite integral domain with unity 1. Let a be any nonzero element of D. We must show that a is a unit. If $a = 1$, a is its own inverse, so we may assume that $a \neq 1$. Now consider the following sequence of elements of D: $a, a^2, a^3, \ldots$. Since D is finite, there must be two positive integers i and j such that $i > j$ and $a^i = a^j$. Then, by cancellation, $a^{i-j} = 1$. Since $a \neq 1$, we know that $i - j > 1$, and we have shown that a^{i-j-1} is the inverse of a. ∎

Corolary:

For every prime p, Z_p, the ring of integers modulo p is a field.

PROOF According to Theorem 13.2, we need only prove that Z_p has no zero-divisors. So, suppose that $a, b \in Z_p$ and $ab = 0$. Then $ab = pk$ for some integer k. But then, by Euclid's Lemma (see Chapter 0), p divides a or p divides b. Thus, in Z_p, $a = 0$ or $b = 0$. ∎

∎ EXAMPLE 9 Field with Nine Elements

Let
$$Z_3[i] = \{a + bi \mid a, b \in Z_3\}$$
$$= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\},$$
where $i^2 = -1$. This is the ring of Gaussian integers modulo 3. Elements are added and multiplied as in the complex numbers, except that the coefficients are reduced modulo 3. In particular, $-1 = 2$. Table 13.1 is the multiplication table for the nonzero elements of $Z_3[i]$. ∎

Table 13.1 Multiplication Table for $Z_3[i]$*

	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$2+i$	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$2i$	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$2+2i$	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

∎ EXAMPLE 10

Let $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Q\}$. It is easy to see that $Q[\sqrt{2}]$ is a ring. Viewed as an element of **R**, the multiplicative inverse of any nonzero element of the form $a + b\sqrt{2}$ is simply $1/(a + b\sqrt{2})$. To verify that $Q[\sqrt{2}]$ is a field, we must show that $1/(a + b\sqrt{2})$ can be written in the form $c + d\sqrt{2}$. In high school algebra, this process is called "rationalizing the denominator." Specifically,

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}}\,\frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

(Note that $a + b\sqrt{2} \neq 0$ guarantees that $a - b\sqrt{2} \neq 0$.) ∎

Characteristics of Rings:

Note that for any element x in $Z_3[i]$, we have $3x = x + x + x = 0$, since addition is done modulo 3. Similarly, in the subring $\{0, 3, 6, 9\}$ of Z_{12}, we have $4x = x + x + x + x = 0$ for all x. This observation motivates the following definition.

Definition Characteristic of a Ring

The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by char R.

Thus, the ring of integers has characteristic 0, and Z_n has characteristic n. An infinite ring can have a nonzero characteristic. Indeed, the ring $Z_2[x]$ of all polynomials with coefficients in Z_2 has characteristic 2. (Addition and multiplication are done as for polynomials with ordinary integer coefficients except that the coefficients are reduced modulo 2.) When a ring has a unity, the task of determining the characteristic is simplified by Theorem 13.3.

Theorem

Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

PROOF If 1 has infinite order, then there is no positive integer n such that $n \cdot 1 = 0$, so R has characteristic 0. Now suppose that 1 has additive order n. Then $n \cdot 1 = 0$, and n is the least positive integer with this property. So, for any x in R, we have

$$\begin{aligned} n \cdot x &= x + x + \cdots + x \ (n \text{ summands}) \\ &= 1x + 1x + \cdots + 1x \ (n \text{ summands}) \end{aligned}$$

$$= (1 + 1 + \cdots + 1)x \ (n \text{ summands})$$
$$= (n \cdot 1)x = 0x = 0.$$

Thus, R has characteristic n. ∎

Theorem

The characteristic of an integral domain is 0 or prime.

PROOF By Theorem 13.3, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that $n = st$, where $1 \le s, t \le n$. Then, by Exercise 15 in Chapter 12,

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1).$$

So, $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since n is the least positive integer with the property that $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus, n is prime. ∎

Table 13.2 Summary of Rings and Their Properties

Ring	Form of Element	Unity	Commutative	Integral Domain	Field	Characteristic
Z	k	1	Yes	Yes	No	0
Z_n, n composite	k	1	Yes	No	No	n
Z_p, p prime	k	1	Yes	Yes	Yes	p
$Z[x]$	$a_nx^n + \cdots + a_1x + a_0$	$f(x) = 1$	Yes	Yes	No	0
$nZ, n > 1$	nk	None	Yes	No	No	0
$M_2(Z)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	No	No	No	0
$M_2(2Z)$	$\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$	None	No	No	No	0
$Z[i]$	$a + bi$	1	Yes	Yes	No	0
$Z_3[i]$	$a + bi$; $a, b \in Z_3$	1	Yes	Yes	Yes	3
$Z[\sqrt{2}]$	$a + b\sqrt{2}$; $a, b \in Z$	1	Yes	Yes	No	0
$Q[\sqrt{2}]$	$a + b\sqrt{2}$; $a, b \in Q$	1	Yes	Yes	Yes	0
$Z \oplus Z$	(a, b)	$(1, 1)$	Yes	No	No	0

Idle:

Normal subgroups play a special role in group theory—they permit us to construct factor groups. In this chapter, we introduce the analogous concepts for rings—ideals and factor rings.

Definition Ideal

A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

So, a subring A of a ring R is an ideal of R if A "absorbs" elements from R—that is, if $rA = \{ra \mid a \in A\} \subseteq A$ and $Ar = \{ar \mid a \in A\} \subseteq A$ for all $r \in R$.

An ideal A of R is called a *proper* ideal of R if A is a proper subset of R. In practice, one identifies ideals with the following test, which is an immediate consequence of the definition of ideal and the subring test given in Theorem 12.3.

Theorem

A nonempty subset A of a ring R is an ideal of R if

1. ***$a - b \in A$ whenever $a, b \in A$.***
2. ***ra and ar are in A whenever $a \in A$ and $r \in R$.***

EXAMPLE 1 For any ring R, $\{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the *trivial* ideal. ∎

EXAMPLE 2 For any positive integer n, the set $nZ = \{0, \pm n, \pm 2n, \ldots\}$ is an ideal of Z. ∎

EXAMPLE 3 Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the *principal ideal generated by a*. (Notice that $\langle a \rangle$ is also the notation we used for the cyclic subgroup generated by a. However, the intended meaning will always be clear from the context.) The assumption that R is commutative is necessary in this example

EXAMPLE 4 Let $\mathbf{R}[x]$ denote the set of all polynomials with real coefficients and let A denote the subset of all polynomials with constant term 0. Then A is an ideal of $\mathbf{R}[x]$ and $A = \langle x \rangle$. ∎

EXAMPLE 5 Let R be a commutative ring with unity and let $a_1, a_2, \ldots, a_n$ belong to R. Then $I = \langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ is an ideal of R called the *ideal generated by* $a_1, a_2, \ldots, a_n$. The verification that I is an ideal is left as an easy exercise (Exercise 3). ∎

EXAMPLE 6 Let $Z[x]$ denote the ring of all polynomials with integer coefficients and let I be the subset of $Z[x]$ of all polynomials with even constant terms. Then I is an ideal of $Z[x]$ and $I = \langle x, 2 \rangle$ (see Exercise 37). ∎

EXAMPLE 7 Let R be the ring of all real-valued functions of a real variable. The subset S of all differentiable functions is a subring of R but not an ideal of R. ∎

Factor Ring:

Let R be a ring and let A be an ideal of R. Since R is a group under addition and A is a normal subgroup of R, we may form the factor group $R/A = \{r + A \mid r \in R\}$. The natural question at this point is: How may we form a ring of this group of cosets? The addition is already taken care of, and, by analogy with groups of cosets, we define the product of two cosets of $s + A$ and $t + A$ as $st + A$. The next theorem shows that this definition works as long as A is an ideal, and not just a subring, of R.

Theorem

Let R be a ring and let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.

PROOF We know that the set of cosets forms a group under addition. Once we know that multiplication is indeed a binary operation on the cosets, it is trivial to check that the multiplication is associative and that multiplication is distributive over addition. Hence, the proof boils down to showing that multiplication is well-defined if and only if A is an ideal of R. To do this, let us suppose that A is an ideal and let $s + A = s' + A$ and $t + A = t' + A$. Then we must show that $st + A = s't' + A$. Well, by definition, $s = s' + a$ and $t = t' + b$, where a and b belong to A. Then

$$st = (s' + a)(t' + b) = s't' + at' + s'b + ab,$$

and so

$$st + A = s't' + at' + s'b + ab + A = s't' + A,$$

since A absorbs $at' + s'b + ab$. Thus, multiplication is well-defined when A is an ideal.

On the other hand, suppose that A is a subring of R that is not an ideal of R. Then there exist elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. For convenience, say $ar \notin A$. Consider the elements $a + A = 0 + A$ and $r + A$. Clearly, $(a + A)(r + A) = ar + A$ but $(0 + A) \cdot (r + A) = 0 \cdot r + A = A$. Since $ar + A \neq A$, the multiplication is not well-defined and the set of cosets is not a ring. ■

■ **EXAMPLE 8** $Z/4Z = \{0 + 4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z\}$. To see how to add and multiply, consider $2 + 4Z$ and $3 + 4Z$.

$$(2 + 4Z) + (3 + 4Z) = 5 + 4Z = 1 + 4 + 4Z = 1 + 4Z,$$
$$(2 + 4Z)(3 + 4Z) = 6 + 4Z = 2 + 4 + 4Z = 2 + 4Z.$$

One can readily see that the two operations are essentially modulo 4 arithmetic. ■

EXAMPLE 9 $2Z/6Z = \{0 + 6Z, 2 + 6Z, 4 + 6Z\}$. Here the operations are essentially modulo 6 arithmetic. For example, $(4 + 6Z) + (4 + 6Z) = 2 + 6Z$ and $(4 + 6Z)(4 + 6Z) = 4 + 6Z$. ∎

Here is a noncommutative example of an ideal and factor ring.

EXAMPLE 10 Let $R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \middle| a_i \in Z \right\}$ and let I be the subset of R consisting of matrices with even entries. It is easy to show that I is indeed an ideal of R (Exercise 21). Consider the factor ring R/I. The interesting question about this ring is: What is its size? We claim R/I has 16 elements; in fact, $R/I = \left\{ \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I \mid r_i \in \{0, 1\} \right\}$. An example illustrates the typical situation. Which of the 16 elements is $\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + I$? Well, observe that $\begin{bmatrix} 7 & 8 \\ 5 & -3 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 8 \\ 4 & -4 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + I$, since an ideal absorbs its own elements. The general case is left to the reader (Exercise 23). ∎

EXAMPLE 11 Consider the factor ring of the Gaussian integers $R = Z[i]/\langle 2 - i\rangle$. What does this ring look like? Of course, the elements of R have the form $a + bi + \langle 2 - i\rangle$, where a and b are integers, but the important question is: What do the *distinct* cosets look like? The fact that $2 - i + \langle 2 - i\rangle = 0 + \langle 2 - i\rangle$ means that *when dealing with coset representatives*, we may treat $2 - i$ as equivalent to 0, so that $2 = i$. For example, the coset $3 + 4i + \langle 2 - i\rangle = 3 + 8 + \langle 2 - i\rangle = 11 + \langle 2 - i\rangle$. Similarly, all the elements of R can be written in the form $a + \langle 2 - i\rangle$, where a is an integer. But we can further reduce the set of distinct coset representatives by observing that *when dealing with coset representatives*, $2 = i$ implies (by squaring both sides) that $4 = -1$ or $5 = 0$. Thus, the coset $3 + 4i + \langle 2 - i\rangle = 11 + \langle 2 - i\rangle = 1 + 5 + 5 + \langle 2 - i\rangle = 1 + \langle 2 - i\rangle$. In this way, we can show that every element of R is equal to one of the following cosets: $0 + \langle 2 - i\rangle$, $1 + \langle 2 - i\rangle$, $2 + \langle 2 - i\rangle$, $3 + \langle 2 - i\rangle$, $4 + \langle 2 - i\rangle$. Is any further reduction possible? To demonstrate that there is not, we will show that these five cosets are distinct. It suffices to show that $1 + \langle 2 - i\rangle$ has additive order 5. Since $5(1 + \langle 2 - i\rangle) = 5 + \langle 2 - i\rangle = 0 + \langle 2 - i\rangle$, $1 + \langle 2 - i\rangle$ has order 1 or 5. If the order is actually 1, then $1 + \langle 2 - i\rangle = 0 + \langle 2 - i\rangle$, so $1 \in \langle 2 - i\rangle$. Thus, $1 = (2 - i)(a + bi) = 2a + b + (-a + 2b)i$ for some integers a and b. But this equation implies that $1 = 2a + b$ and $0 = -a + 2b$, and solving these simultaneously yields $b = 1/5$, which is a contradiction. It should be clear that the ring R is essentially the same as the field Z_5. ■

■ **EXAMPLE 12** Let $\mathbf{R}[x]$ denote the ring of polynomials with real coefficients and let $\langle x^2 + 1\rangle$ denote the principal ideal generated by $x^2 + 1$; that is,

$$\langle x^2 + 1\rangle = \{f(x)(x^2 + 1) \mid f(x) \in \mathbf{R}[x]\}.$$

Then

$$\begin{aligned}\mathbf{R}[x]/\langle x^2 + 1\rangle &= \{g(x) + \langle x^2 + 1\rangle \mid g(x) \in \mathbf{R}[x]\}\\ &= \{ax + b + \langle x^2 + 1\rangle \mid a, b \in \mathbf{R}\}.\end{aligned}$$

To see this last equality, note that if $g(x)$ is any member of $\mathbf{R}[x]$, then we may write $g(x)$ in the form $q(x)(x^2 + 1) + r(x)$, where $q(x)$ is the quotient and $r(x)$ is the remainder upon dividing $g(x)$ by $x^2 + 1$. In particular, $r(x) = 0$ or the degree of $r(x)$ is less than 2, so that $r(x) = ax + b$ for some a and b in $\mathbf{R}$. Thus,

$$\begin{aligned}g(x) + \langle x^2 + 1\rangle &= q(x)(x^2 + 1) + r(x) + \langle x^2 + 1\rangle\\ &= r(x) + \langle x^2 + 1\rangle,\end{aligned}$$

since the ideal $\langle x^2 + 1\rangle$ absorbs the term $q(x)(x^2 + 1)$.

How is multiplication done? Since

$$x^2 + 1 + \langle x^2 + 1\rangle = 0 + \langle x^2 + 1\rangle,$$

one should think of $x^2 + 1$ as 0 or, equivalently, as $x^2 = -1$. So, for example,

$$(x + 3 + \langle x^2 + 1\rangle) \cdot (2x + 5 + \langle x^2 + 1\rangle)$$
$$= 2x^2 + 11x + 15 + \langle x^2 + 1\rangle = 11x + 13 + \langle x^2 + 1\rangle.$$

In view of the fact that the elements of this ring have the form $ax + b + \langle x^2 + 1\rangle$, where $x^2 + \langle x^2 + 1\rangle = -1 + \langle x^2 + 1\rangle$, it is perhaps not surprising that this ring turns out to be algebraically the same ring as the ring of complex numbers. This observation was first made by Cauchy in 1847. ■

Prime ideal and Maximal ideal:

Definition Prime Ideal, Maximal Ideal

A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal* ideal of a commutative ring R is a *proper* ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

So, the only ideal that properly contains a maximal ideal is the entire ring. The motivation for the definition of a prime ideal comes from the integers.

■ **EXAMPLE 13** Let n be an integer greater than 1. Then, in the ring of integers, the ideal nZ is prime if and only if n is prime (Exercise 9). ($\{0\}$ is also a prime ideal of Z.) ■

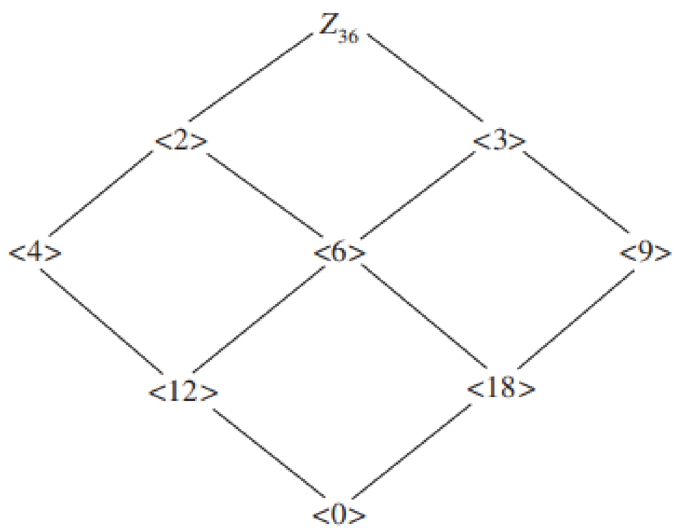
■ **EXAMPLE 14** The lattice of ideals of Z_{36} (Figure 14.1) shows that only $\langle 2\rangle$ and $\langle 3\rangle$ are maximal ideals. ■

■ **EXAMPLE 15** The ideal $\langle x^2 + 1\rangle$ is maximal in $\mathbf{R}[x]$. To see this, assume that A is an ideal of $\mathbf{R}[x]$ that properly contains $\langle x^2 + 1\rangle$. We will prove that $A = \mathbf{R}[x]$ by showing that A contains some nonzero real number c. [This is the constant polynomial $h(x) = c$ for all x.] Then $1 = (1/c)c \in A$ and therefore, by Exercise 15, $A = \mathbf{R}[x]$. To this end, let $f(x) \in A$, but $f(x) \notin \langle x^2 + 1\rangle$. Then

$$f(x) = q(x)(x^2 + 1) + r(x),$$

where $r(x) \neq 0$ and the degree of $r(x)$ is less than 2. It follows that $r(x) = ax + b$, where a and b are not both 0, and

$$ax + b = r(x) = f(x) - q(x)(x^2 + 1) \in A.$$



Thus,

$$a^2x^2 - b^2 = (ax + b)(ax - b) \in A \quad \text{and} \quad a^2(x^2 + 1) \in A.$$

So,

$$0 \neq a^2 + b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A. \quad ■$$

■ **EXAMPLE 16** The ideal $\langle x^2 + 1 \rangle$ is not prime in $Z_2[x]$, since it contains $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ but does not contain $x + 1$. ■

Theorem

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime.

PROOF Suppose that R/A is a field and B is an ideal of R that properly contains A. Let $b \in B$ but $b \notin A$. Then $b + A$ is a nonzero element of R/A and, therefore, there exists an element $c + A$ such that

$(b + A) \cdot (c + A) = 1 + A$, the multiplicative identity of R/A. Since $b \in B$, we have $bc \in B$. Because

$$1 + A = (b + A)(c + A) = bc + A,$$

we have $1 - bc \in A \subset B$. So, $1 = (1 - bc) + bc \in B$. By Exercise 15, $B = R$. This proves that A is maximal.

Now suppose that A is maximal and let $b \in R$ but $b \notin A$. It suffices to show that $b + A$ has a multiplicative inverse. (All other properties for a field follow trivially.) Consider $B = \{br + a \mid r \in R, a \in A\}$. This is an ideal of R that properly contains A (Exercise 25). Since A is maximal, we must have $B = R$. Thus, $1 \in B$, say, $1 = bc + a'$, where $a' \in A$. Then

$$1 + A = bc + a' + A = bc + A = (b + A)(c + A).$$

EXAMPLE 17 The ideal $\langle x \rangle$ is a prime ideal in $Z[x]$ but not a maximal ideal in $Z[x]$. To verify this, we begin with the observation that $\langle x \rangle = \{f(x) \in Z[x] \mid f(0) = 0\}$ (see Exercise 29). Thus, if $g(x)h(x) \in \langle x \rangle$, then $g(0)h(0) = 0$. And since $g(0)$ and $h(0)$ are integers, we have $g(0) = 0$ or $h(0) = 0$.

To see that $\langle x \rangle$ is not maximal, we simply note that $\langle x \rangle \subset \langle x, 2 \rangle \subset Z[x]$ (see Exercise 37).

UNIT-II

SYLLABUS

Ring homomorphisms - Properties of ring homomorphisms - Isomorphism theorems I, II and III - Field of quotients.

Definitions Ring Homomorphism, Ring Isomorphism

A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$$\phi(a + b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

EXAMPLE 1 For any positive integer n, the mapping $k \to k \bmod n$ is a ring homomorphism from Z onto Z_n (see Exercise 9 in Chapter 0). This mapping is called the *natural homomorphism* from Z to Z_n. ▮

EXAMPLE 2 The mapping $a + bi \to a - bi$ is a ring isomorphism from the complex numbers onto the complex numbers (see Exercise 35 in Chapter 6). ▮

EXAMPLE 3 Let $\mathbf{R}[x]$ denote the ring of all polynomials with real coefficients. The mapping $f(x) \to f(1)$ is a ring homomorphism from $\mathbf{R}[x]$ onto $\mathbf{R}$. ▮

EXAMPLE 4 The correspondence ϕ: $x \to 5x$ from Z_4 to Z_{10} is a ring homomorphism. Although showing that $\phi(x + y) = \phi(x) + \phi(y)$ appears to be accomplished by the simple statement that $5(x + y) = 5x + 5y$, we must bear in mind that the addition on the left is done modulo 4, whereas the addition on the right and the multiplication on both sides are done modulo 10. An analogous difficulty arises in showing that ϕ preserves multiplication. So, to verify that ϕ preserves both operations, we write $x + y = 4q_1 + r_1$ and $xy = 4q_2 + r_2$, where $0 \leq r_1 < 4$ and $0 \leq r_2 < 4$. Then $\phi(x + y) = \phi(r_1) = 5r_1 = 5(x + y - 4q_1) = 5x + 5y - 20q_1 = 5x + 5y = \phi(x) + \phi(y)$ in Z_{10}. Similarly, using the fact that $5 \cdot 5 = 5$ in Z_{10}, we have $\phi(xy) = \phi(r_2) = 5r_2 = 5(xy - 4q_2) = 5xy - 20q_2 = (5 \cdot 5)xy = 5x5y = \phi(x)\phi(y)$ in Z_{10}. ▮

EXAMPLE 5 We determine all ring homomorphisms from Z_{12} to Z_{30}. By Example 10 in Chapter 10, the only group homomorphisms from Z_{12} to Z_{30} are $x \to ax$, where $a = 0, 15, 10, 20, 5$, or 25. But, since $1 \cdot 1 = 1$ in Z_{12}, we must have $a \cdot a = a$ in Z_{30}. This requirement rules out 20 and 5 as possibilities for a. Finally, simple calculations show that each of the remaining four choices does yield a ring homomorphism. ∎

Properties of Ring Homomorphisms

Theorem 15.1 Properties of Ring Homomorphisms

Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1. *For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.*
2. *$\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.*
3. *If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.*
4. *$\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.*
5. *If R is commutative, then $\phi(R)$ is commutative.*
6. *If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.*
7. *ϕ is an isomorphism if and only if ϕ is onto and Ker $\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.*
8. *If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.*

Theorem 15.2 Kernels Are Ideals

Let ϕ be a ring homomorphism from a ring R to a ring S. Then Ker $\phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.

Theorem 15.3 First Isomorphism Theorem for Rings

Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\text{Ker } \phi$ to $\phi(R)$, given by $r + \text{Ker } \phi \to \phi(r)$, is an isomorphism. In symbols, $R/\text{Ker } \phi \approx \phi(R)$.

Theorem 15.4 Ideals Are Kernels

Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.

The homomorphism from R to R/A given in Theorem 15.4 is called the *natural homomorphism* from R to R/A. Theorem 15.3 is often referred to as the Fundamental Theorem of Ring Homomorphisms.

In Example 17 in Chapter 14 we gave a direct proof that $\langle x \rangle$ is a prime ideal of $Z[x]$ but not a maximal ideal. In the following example we illustrate a better way to do this kind of problem.

Theorem 15.5 Homomorphism from Z to a Ring with Unity

Let R be a ring with unity 1. The mapping $\phi: Z \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

PROOF Since the multiplicative group property $a^{m+n} = a^m a^n$ translates to $(m + n)a = ma + na$ when the operation is addition, we have $\phi(m + n) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1$. So, ϕ preserves addition.

That ϕ also preserves multiplication follows from Exercise 15 in Chapter 12, which says that $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$ for all integers m and n. Thus, $\phi(mn) = (mn) \cdot 1 = (mn) \cdot ((1)(1)) = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n)$. So, ϕ preserves multiplication as well. ∎

Corollary 1 A Ring with Unity Contains Z_n or Z

If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to Z_n. If the characteristic of R is 0, then R contains a subring isomorphic to Z.

PROOF Let 1 be the unity of R and let $S = \{k \cdot 1 \mid k \in Z\}$. Theorem 15.5 shows that the mapping ϕ from Z to S given by $\phi(k) = k \cdot 1$ is a homomorphism, and by the First Isomorphism Theorem for rings, we have $Z/\text{Ker } \phi \approx S$. But, clearly, $\text{Ker } \phi = \langle n \rangle$, where n is the additive order of 1 and, by Theorem 13.3, n is also the characteristic of R. So, when R has characteristic n, $S \approx Z/\langle n \rangle \approx Z_n$. When R has characteristic 0, $S \approx Z/\langle 0 \rangle \approx Z$. ∎

Corollary 2 Z_m Is a Homomorphic Image of Z

For any positive integer m, the mapping of $\phi: Z \to Z_m$ given by $x \to x \bmod m$ is a ring homomorphism.

PROOF This follows directly from the statement of Theorem 15.5, since in the ring Z_m, the integer x mod m is $x \cdot 1$. (For example, in Z_3, if $x = 5$, we have $5 \cdot 1 = 1 + 1 + 1 + 1 + 1 = 2$.) ∎

Corollary 3 A Field Contains Z_p or Q (Steinitz, 1910)

If F is a field of characteristic p, then F contains a subfield isomorphic to Z_p. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

PROOF By Corollary 1, F contains a subring isomorphic to Z_p if F has characteristic p, and F has a subring S isomorphic to Z if F has characteristic 0. In the latter case, let

$$T = \{ab^{-1} \mid a, b \in S, b \neq 0\}.$$

Then T is isomorphic to the rationals (Exercise 63). ∎

Since the intersection of all subfields of a field is itself a subfield (Exercise 11), every field has a smallest subfield (that is, a subfield that is contained in every subfield). This subfield is called the *prime subfield* of the field. It follows from Corollary 3 that the prime subfield of a field of characteristic p is isomorphic to Z_p, whereas the prime subfield of a field of characteristic 0 is isomorphic to Q. (See Exercise 67.)

The Field of Quotients

Theorem 15.6 Field of Quotients

Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

PROOF Let $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. We define an equivalence relation on S by $(a, b) \equiv (c, d)$ if $ad = bc$ (compare with Example 17 in Chapter 0). Now, let F be the set of equivalence classes of S under the relation $\equiv$ and denote the equivalence class that contains (x, y) by x/y. We define addition and multiplication on F by

$$a/b + c/d = (ad + bc)/(bd) \qquad \text{and} \qquad a/b \cdot c/d = (ac)/(bd).$$

(Notice that here we need the fact that D is an integral domain to ensure that multiplication is closed; that is, $bd \neq 0$ whenever $b \neq 0$ and $d \neq 0$.)

Since there are many representations of any particular element of F (just as in the rationals, we have $1/2 = 3/6 = 4/8$), we must show that these two operations are well-defined. To do this, suppose that $a/b = a'/b'$ and $c/d = c'/d'$, so that $ab' = a'b$ and $cd' = c'd$. It then follows that

$$\begin{aligned}(ad + bc)b'd' &= adb'd' + bcb'd' = (ab')dd' + (cd')bb' \\ &= (a'b)dd' + (c'd)bb' = a'd'bd + b'c'bd \\ &= (a'd' + b'c')bd.\end{aligned}$$

Thus, by definition, we have

$$(ad + bc)/(bd) = (a'd' + b'c')/(b'd'),$$

and, therefore, addition is well-defined. We leave the verification that multiplication is well-defined as an exercise (Exercise 55). That F is a field is straightforward. Let 1 denote the unity of D. Then $0/1$ is the additive identity of F. The additive inverse of a/b is $-a/b$; the multiplicative inverse of a nonzero element a/b is b/a. The remaining field properties can be checked easily.

Finally, the mapping $\phi: D \to F$ given by $x \to x/1$ is a ring isomorphism from D to $\phi(D)$ (see Exercise 7). ■

EXAMPLE 11 Let $D = Z[x]$. Then the field of quotients of D is $\{f(x)/g(x) \mid f(x), g(x) \in D$, where $g(x)$ is not the zero polynomial$\}$. ∎

When F is a field, the field of quotients of $F[x]$ is traditionally denoted by $F(x)$.

EXAMPLE 12 Let p be a prime. Then $Z_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in Z_p[x], g(x) \neq 0\}$ is an infinite field of characteristic p. ∎

UNIT-III

SYLLABUS

Vector spaces - Subspaces - Algebra of subspaces - Quotient spaces - Linear combination of vectors - Linear span - Linear independence - Basis and dimension - Dimension of subspaces.

Vector Spaces

DEFINITION A nonempty set V is said to be a *vector space* over a field F if V is an abelian group under an operation which we denote by $+$, and if for every $\alpha \in F$, $v \in V$ there is defined an element, written αv, in V subject to

1. $\alpha(v + w) = \alpha v + \alpha w$;
2. $(\alpha + \beta)v = \alpha v + \beta v$;
3. $\alpha(\beta v) = (\alpha\beta)v$;
4. $1v = v$;

for all $\alpha, \beta \in F$, $v, w \in V$ (where the 1 represents the unit element of F under multiplication).

Example 4.1.1 Let F be a field and let K be a field which contains F as a subfield. We consider K as a vector space over F, using as the $+$ of the vector space the addition of elements of K, and by defining, for $\alpha \in F$, $v \in K$, αv to be the products of α and v as elements in the field K. Axioms 1, 2, 3 for a vector space are then consequences of the right-distributive law, left-distributive law, and associative law, respectively, which hold for K as a ring.

Example 4.1.2 Let F be a field and let V be the totality of all ordered n-tuples, $(\alpha_1, \ldots, \alpha_n)$ where the $\alpha_i \in F$. Two elements $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ of V are declared to be equal if and only if $\alpha_i = \beta_i$ for each $i = 1, 2, \ldots, n$. We now introduce the requisite operations in V to make of it a vector space by defining:

1. $(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$.
2. $\gamma(\alpha_1, \ldots, \alpha_n) = (\gamma\alpha_1, \ldots, \gamma\alpha_n)$ for $\gamma \in F$.

Example 4.1.3 Let F be any field and let $V = F[x]$, the set of polynomials in x over F. We choose to ignore, at present, the fact that in $F[x]$ we can multiply any two elements, and merely concentrate on the fact that two polynomials can be added and that a polynomial can always be multiplied by an element of F. With these natural operations $F[x]$ is a vector space over F.

Example 4.1.4 In $F[x]$ let V_n be the set of all polynomials of degree less than n. Using the natural operations for polynomials of addition and multiplication, V_n is a vector space over F.

What is the relation of Example 4.1.4 to Example 4.1.2? Any element of V_n is of the form $\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1}$, where $\alpha_i \in F$; if we map this element onto the element $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ in $F^{(n)}$ we could reasonably expect, once homomorphism and isomorphism have been defined, to find that V_n and $F^{(n)}$ are isomorphic as vector spaces.

DEFINITION If V is a vector space over F and if $W \subset V$, then W is a *subspace* of V if under the operations of V, W, itself, forms a vector space over F. Equivalently, W is a subspace of V whenever $w_1, w_2 \in W$, $\alpha, \beta \in F$ implies that $\alpha w_1 + \beta w_2 \in W$.

DEFINITION If U and V are vector spaces over F then the mapping T of U into V is said to be a *homomorphism* if

1. $(u_1 + u_2)T = u_1T + u_2T$;
2. $(\alpha u_1)T = \alpha(u_1T)$;

for all $u_1, u_2 \in U$, and all $\alpha \in F$.

As in our previous models, a homomorphism is a mapping preserving all the algebraic structure of our system.

LEMMA 4.1.1 *If V is a vector space over F then*

1. $\alpha 0 = 0$ *for* $\alpha \in F$.
2. $ov = 0$ *for* $v \in V$.
3. $(-\alpha)v = -(\alpha v)$ *for* $\alpha \in F$, $v \in V$.
4. If $v \neq 0$, *then* $\alpha v = 0$ *implies that* $\alpha = o$.

Proof. The proof is very easy and follows the lines of the analogous results proved for rings; for this reason we give it briefly and with few explanations.

- Since $\alpha 0 = \alpha(0 + 0) = \alpha 0 + \alpha 0$, we get $\alpha 0 = 0$.
- Since $ov = (o + o)v = ov + ov$ we get $ov = 0$.

3. Since $0 = (\alpha + (-\alpha))v = \alpha v + (-\alpha)v$, $(-\alpha)v = -(\alpha v)$.
4. If $\alpha v = 0$ and $\alpha \neq o$ then

$$0 = \alpha^{-1}0 = \alpha^{-1}(\alpha v) = (\alpha^{-1}\alpha)v = 1v = v.$$

The lemma just proved shows that multiplication by the zero of V or of F always leads us to the zero of V. Thus there will be no danger of confusion in using the same symbol for both of these, and we henceforth will merely use the symbol 0 to represent both of them.

Let V be a vector space over F and let W be a subspace of V. Considering these merely as abelian groups construct the quotient group V/W; its elements are the cosets $v + W$ where $v \in V$. The commutativity of the addition, from what we have developed in Chapter 2 on group theory, assures us that V/W is an abelian group. We intend to make of it a vector space. If $\alpha \in F$, $v + W \in V/W$, define $\alpha(v + W) = \alpha v + W$. As is usual, we must first show that this product is well defined; that is, if $v + W = v' + W$ then $\alpha(v + W) = \alpha(v' + W)$. Now, because $v + W = v' + W$, $v - v'$ is in W; since W is a subspace, $\alpha(v - v')$ must also be in W. Using part 3 of Lemma 4.1.1 (see Problem 1) this says that $\alpha v - \alpha v' \in W$ and so $\alpha v + W = \alpha v' + W$. Thus $\alpha(v + W) = \alpha v + W = \alpha v' + W = \alpha(v' + W)$; the product has been shown to be well defined. The verification of the vector-space axioms for V/W is routine and we leave it as an exercise. We have shown

LEMMA 4.1.2 *If V is a vector space over F and if W is a subspace of V, then V/W is a vector space over F, where, for $v_1 + W$, $v_2 + W \in V/W$ and $\alpha \in F$,*

1. $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$.
2. $\alpha(v_1 + W) = \alpha v_1 + W$.

V/W is called the *quotient space* of V by W.

Without further ado we now state the first homomorphism theorem for vector spaces; we give no proofs but refer the reader back to the proof of Theorem 2.7.1.

THEOREM 4.1.1 *If T is a homomorphism of U onto V with kernel W, then V is isomorphic to U/W. Conversely, if U is a vector space and W a subspace of U, then there is a homomorphism of U onto U/W.*

DEFINITION Let V be a vector space over F and let $U_1, \ldots, U_n$ be subspaces of V. V is said to be the *internal direct sum* of $U_1, \ldots, U_n$ if every element $v \in V$ can be written in one and only one way as $v = u_1 + u_2 + \cdots + u_n$ where $u_i \in U_i$.

Given any finite number of vector spaces over F, $V_1, \ldots, V_n$, consider the set V of all ordered n-tuples $(v_1, \ldots, v_n)$ where $v_i \in V_i$. We declare two elements $(v_1, \ldots, v_n)$ and $(v_1', \ldots, v_n')$ of V to be equal if and only if for each i, $v_i = v_i'$. We add two such elements by defining $(v_1, \ldots, v_n) + (w_1, \ldots, w_n)$ to be $(v_1 + w_1, v_2 + w_2, \ldots, v_n + w_n)$. Finally, if $\alpha \in F$ and $(v_1, \ldots, v_n) \in V$ we define $\alpha(v_1, \ldots, v_n)$ to be $(\alpha v_1, \alpha v_2, \ldots, \alpha v_n)$. To check that the axioms for a vector space hold for V with its operations as defined above is straightforward. Thus V itself is a vector space over F. We call V the *external direct sum* of $V_1, \ldots, V_n$ and denote it by writing $V = V_1 \oplus \cdots \oplus V_n$.

THEOREM 4.1.2 *If V is the internal direct sum of $U_1, \ldots, U_n$, then V is isomorphic to the external direct sum of $U_1, \ldots, U_n$.*

Proof. Given $v \in V$, v can be written, by assumption, in one and only one way as $v = u_1 + u_2 + \cdots + u_n$ where $u_i \in U_i$; define the mapping T of V into $U_1 \oplus \cdots \oplus U_n$ by $vT = (u_1, \ldots, u_n)$. Since v has a unique representation of this form, T is well defined. It clearly is onto, for the arbitrary element $(w_1, \ldots, w_n) \in U_1 \oplus \cdots \oplus U_n$ is wT where $w = w_1 + \cdots + w_n \in V$. We leave the proof of the fact that T is one-to-one and a homomorphism to the reader.

Linear Independence and Bases

DEFINITION If V is a vector space over F and if $v_1, \ldots, v_n \in V$ then any element of the form $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$, where the $\alpha_i \in F$, is a *linear combination* over F of $v_1, \ldots, v_n$.

DEFINITION If S is a nonempty subset of the vector space V, then $L(S)$, the *linear span* of S, is the set of all linear combinations of finite sets of elements of S.

LEMMA 4.2.1 *$L(S)$ is a subspace of V.*

Proof. If v and w are in $L(S)$, then $v = \lambda_1 s_1 + \cdots + \lambda_n s_n$ and $w = \mu_1 t_1 + \cdots + \mu_m t_m$, where the λ's and μ's are in F and the s_i and t_i are all in S. Thus, for $\alpha, \beta \in F$, $\alpha v + \beta w = \alpha(\lambda_1 s_1 + \cdots + \lambda_n s_n) + \beta(\mu_1 t_1 + \cdots + \mu_m t_m) = (\alpha\lambda_1)s_1 + \cdots + (\alpha\lambda_n)s_n + (\beta\mu_1)t_1 + \cdots + (\beta\mu_m)t_m$ and so is again in $L(S)$. $L(S)$ has been shown to be a subspace of V.

LEMMA 4.2.2 *If S, T are subsets of V, then*

1. $S \subset T$ *implies* $L(S) \subset L(T)$.
2. $L(S \cup T) = L(S) + L(T)$.
3. $L(L(S)) = L(S)$.

DEFINITION The vector space V is said to be *finite-dimensional* (over F) if there is a *finite* subset S in V such that $V = L(S)$.

Note that $F^{(n)}$ is finite-dimensional over F, for if S consists of the n vectors $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)$, then $V = L(S)$.

DEFINITION If V is a vector space and if $v_1, \ldots, v_n$ are in V, we say that they are *linearly dependent* over F if there exist elements $\lambda_1, \ldots, \lambda_n$ in F, not all of them 0, such that $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$.

LEMMA 4.2.3 *If $v_1, \ldots, v_n \in V$ are linearly independent, then every element in their linear span has a unique representation in the form $\lambda_1 v_1 + \cdots + \lambda_n v_n$ with the $\lambda_i \in F$.*

Proof. By definition, every element in the linear span is of the form $\lambda_1 v_1 + \cdots + \lambda_n v_n$. To show uniqueness we must demonstrate that if $\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n$ then $\lambda_1 = \mu_1, \lambda_2 = \mu_2, \ldots, \lambda_n = \mu_n$. But if $\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n$, then we certainly have $(\lambda_1 - \mu_1)v_1 + (\lambda_2 - \mu_2)v_2 + \cdots + (\lambda_n - \mu_n)v_n = 0$, which by the linear independence of $v_1, \ldots, v_n$ forces $\lambda_1 - \mu_1 = 0$, $\lambda_2 - \mu_2 = 0, \ldots, \lambda_n - \mu_n = 0$.

THEOREM 4.2.1 *If $v_1, \ldots, v_n$ are in V then either they are linearly independent or some v_k is a linear combination of the preceding ones, $v_1, \ldots, v_{k-1}$.*

Proof. If $v_1, \ldots, v_n$ are linearly independent there is, of course, nothing to prove. Suppose then that $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ where not all the α's are 0. Let k be the largest integer for which $\alpha_k \neq 0$. Since $\alpha_i = 0$ for $i > k$, $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$ which, since $\alpha_k \neq 0$, implies that $v_k = \alpha_k^{-1}(-\alpha_1 v_1 - \alpha_2 v_2 - \cdots - \alpha_{k-1} v_{k-1}) = (-\alpha_k^{-1}\alpha_1)v_1 + \cdots + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$. Thus v_k is a linear combination of its predecessors.

COROLLARY 1 *If $v_1, \ldots, v_n$ in V have W as linear span and if $v_1, \ldots, v_k$ are linearly independent, then we can find a subset of $v_1, \ldots, v_n$ of the form $v_1, v_2, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ consisting of linearly independent elements whose linear span is also W.*

Proof. If $v_1, \ldots, v_n$ are linearly independent we are done. If not, weed out from this set the first v_j, which is a linear combination of its predecessors. Since $v_1, \ldots, v_k$ are linearly independent, $j > k$. The subset so constructed, $v_1, \ldots, v_k, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$ has $n - 1$ elements. Clearly its linear span is contained in W. However, we claim that it is actually equal to W; for, given $w \in W$, w can be written as a linear combination of $v_1, \ldots, v_n$. But in this linear combination we can replace v_j by a linear combination of $v_1, \ldots, v_{j-1}$. That is, w is a linear combination of $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$.

Continuing this weeding out process, we reach a subset $v_1, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ whose linear span is still W but in which no element is a linear combination of the preceding ones. By Theorem 4.2.1 the elements $v_1, \ldots, v_k, v_{i_1}, \ldots, v_{i_r}$ must be linearly independent.

COROLLARY 2 *If V is a finite-dimensional vector space, then it contains a finite set $v_1, \ldots, v_n$ of linearly independent elements whose linear span is V.*

Proof. Since V is finite-dimensional, it is the linear span of a finite number of elements $u_1, \ldots, u_m$. By Corollary 1 we can find a subset of these, denoted by $v_1, \ldots, v_n$, consisting of linearly independent elements whose linear span must also be V.

DEFINITION A subset S of a vector space V is called a *basis* of V if S consists of linearly independent elements (that is, any finite number of elements in S is linearly independent) and $V = L(S)$.

COROLLARY 3 *If V is a finite-dimensional vector space and if $u_1, \ldots, u_m$ span V then some subset of $u_1, \ldots, u_m$ forms a basis of V.*

Corollary 3 asserts that a finite-dimensional vector space has a basis containing a finite number of elements $v_1, \ldots, v_n$. Together with Lemma 4.2.3 this tells us that every element in V has a unique representation in the form $\alpha_1 v_1 + \cdots + \alpha_n v_n$ with $\alpha_1, \ldots, \alpha_n$ in F.

Let us see some of the heuristic implications of these remarks. Suppose that V is a finite-dimensional vector space over F; as we have seen above, V has a basis $v_1, \ldots, v_n$. Thus every element $v \in V$ has a unique representation in the form $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$. Let us map V into $F^{(n)}$ by defining the image of $\alpha_1 v_1 + \cdots + \alpha_n v_n$ to be $(\alpha_1, \ldots, \alpha_n)$. By the uniqueness of representation in this form, the mapping is well defined, one-to-one, and onto; it can be shown to have all the requisite properties of an isomorphism. Thus V is isomorphic to $F^{(n)}$ for some n, where in fact n is the number of elements in some basis of V over F. If some other basis of V should have m elements, by the same token V would be isomorphic to $F^{(m)}$. Since both $F^{(n)}$ and $F^{(m)}$ would now be isomorphic to V, they would be isomorphic to each other.

LEMMA 4.2.4 *If $v_1, \ldots, v_n$ is a basis of V over F and if $w_1, \ldots, w_m$ in V are linearly independent over F, then $m \leq n$.*

Proof. Every vector in V, so in particular w_m, is a linear combination of $v_1, \ldots, v_n$. Therefore the vectors $w_m, v_1, \ldots, v_n$ are linearly dependent.

Moreover, they span V since $v_1, \ldots, v_n$ already do so. Thus some proper subset of these $w_m, v_{i_1}, \ldots, v_{i_k}$ with $k \leq n - 1$ forms a basis of V. We have "traded off" one w, in forming this new basis, for at least one v_i. Repeat this procedure with the set $w_{m-1}, w_m, v_{i_1}, \ldots, v_{i_k}$. From this linearly dependent set, by Corollary 1 to Theorem 4.2.1, we can extract a basis of the form $w_{m-1}, w_m, v_{j_1}, \ldots, v_{j_s}$, $s \leq n - 2$. Keeping up this procedure we eventually get down to a basis of V of the form $w_2, \ldots, w_{m-1}, w_m, v_\alpha, v_\beta \ldots$; since w_1 is not a linear combination of $w_2, \ldots, w_{m-1}$, the above basis must actually include some v. To get to this basis we have introduced $m - 1$ w's, each such introduction having cost us at least one v, and yet there is a v left. Thus $m - 1 \leq n - 1$ and so $m \leq n$.

COROLLARY 1 *If V is finite-dimensional over F then any two bases of V have the same number of elements.*

Proof. Let $v_1, \ldots, v_n$ be one basis of V over F and let $w_1, \ldots, w_m$ be another. In particular, $w_1, \ldots, w_m$ are linearly independent over F whence, by Lemma 4.2.4, $m \leq n$. Now interchange the roles of the v's and w's and we obtain that $n \leq m$. Together these say that $n = m$.

COROLLARY 2 *$F^{(n)}$ is isomorphic $F^{(m)}$ if and only if $n = m$.*

Proof. $F^{(n)}$ has, as one basis, the set of n vectors, $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)$. Likewise $F^{(m)}$ has a basis containing m vectors. An isomorphism maps a basis onto a basis (Problem 4, end of this section), hence, by Corollary 1, $m = n$.

COROLLARY 3 *If V is finite-dimensional over F then V is isomorphic to $F^{(n)}$ for a unique integer n; in fact, n is the number of elements in any basis of V over F.*

DEFINITION The integer n in Corollary 3 is called the *dimension* of V over F.

The dimension of V over F is thus the number of elements in any basis of V over F.

COROLLARY 4 *Any two finite-dimensional vector spaces over F of the same dimension are isomorphic.*

Proof. If this dimension is n, then each is isomorphic to $F^{(n)}$, hence they are isomorphic to each other.

LEMMA 4.2.5 *If V is finite-dimensional over F and if $u_1, \ldots, u_m \in V$ are linearly independent, then we can find vectors $u_{m+1}, \ldots, u_{m+r}$ in V such that $u_1, \ldots, u_m, u_{m+1}, \ldots, u_{m+r}$ is a basis of V.*

Proof. Since V is finite-dimensional it has a basis; let $v_1, \ldots, v_n$ be a basis of V. Since these span V, the vectors $u_1, \ldots, u_m, v_1, \ldots, v_n$ also span V. By Corollary 1 to Theorem 4.2.1 there is a subset of these of the form $u_1, \ldots, u_m, v_{i_1}, \ldots, v_{i_r}$ which consists of linearly independent elements which span V. To prove the lemma merely put $u_{m+1} = v_{i_1}, \ldots, u_{m+r} = v_{i_r}$.

LEMMA 4.2.6 *If V is finite-dimensional and if W is a subspace of V, then W is finite-dimensional*, $\dim W \le \dim V$ *and* $\dim V/W = \dim V - \dim W$.

Proof. By Lemma 4.2.4, if $n = \dim V$ then any $n + 1$ elements in V are linearly dependent; in particular, any $n + 1$ elements in W are linearly dependent. Thus we can find a largest set of linearly independent elements in W, $w_1, \ldots, w_m$ and $m \le n$. If $w \in W$ then $w_1, \ldots, w_m, w$ is a linearly dependent set, whence $\alpha w + \alpha_1 w_1 + \cdots + \alpha_m w_m = 0$, and not all of the α_i's are 0. If $\alpha = 0$, by the linear independence of the w_i we would get that each $\alpha_i = 0$, a contradiction. Thus $\alpha \ne 0$, and so $w = -\alpha^{-1}(\alpha_1 w_1 + \cdots + \alpha_m w_m)$. Consequently, $w_1, \ldots, w_m$ span W; by this, W is finite-dimensional over F, and furthermore, it has a basis of m elements, where $m \le n$. From the definition of dimension it then follows that $\dim W \le \dim V$.

Now, let $w_1, \ldots, w_m$ be a basis of W. By Lemma 4.2.5, we can fill this out to a basis, $w_1, \ldots, w_m, v_1, \ldots, v_r$ of V, where $m + r = \dim V$ and $m = \dim W$.

Let $\bar{v}_1, \ldots, \bar{v}_r$ be the images, in $\bar{V} = V/W$, of $v_1, \ldots, v_r$. Since any vector $v \in V$ is of the form $v = \alpha_1 w_1 + \cdots + \alpha_m w_m + \beta_1 v_1 + \cdots + \beta_r v_r$, then $\bar{v}$, the image of v, is of the form $\bar{v} = \beta_1 \bar{v}_1 + \cdots + \beta_r \bar{v}_r$ (since $\bar{w}_1 = \bar{w}_2 = \cdots = \bar{w}_m = 0$). Thus $\bar{v}_1, \ldots, \bar{v}_r$ span V/W. We claim that they are linearly independent, for if $\gamma_1 \bar{v}_1 + \cdots + \gamma_r \bar{v}_r = 0$ then $\gamma_1 v_1 + \cdots + \gamma_r v_r \in W$, and so $\gamma_1 v_1 + \cdots + \gamma_r v_r = \lambda_1 w_1 + \cdots + \lambda_m w_m$, which, by the linear independence of the set $w_1, \ldots, w_m, v_1, \ldots, v_r$ forces $\gamma_1 = \cdots = \gamma_r = \lambda_1 = \cdots = \lambda_m = 0$. We have shown that V/W has a basis of r elements, and so, $\dim V/W = r = \dim V - m = \dim V - \dim W$.

COROLLARY *If A and B are finite-dimensional subspaces of a vector space V, then $A + B$ is finite-dimensional and* $\dim(A + B) = \dim(A) + \dim(B) - \dim(A \cap B)$.

Proof. By the result of Problem 13 at the end of Section 4.1,

$$\frac{A + B}{B} \approx \frac{A}{A \cap B},$$

and since A and B are finite-dimensional, we get that and since A and B are finite-dimensional, we get that

$$\dim(A+B) - \dim B = \dim\left(\frac{A+B}{B}\right) = \dim\left(\frac{A}{A \cap B}\right)$$
$$= \dim A - \dim(A \cap B).$$

UNIT-IV

SYLLABUS

Linear transformations - Null space - Range - Rank and nullity of a linear transformation – Matrix representation of a linear transformation - Algebra of linear transformations.

Linear Transformations

DEFINITION If U and V are vector spaces over F then the mapping T of U into V is said to be a *homomorphism* if

1. $(u_1 + u_2)T = u_1T + u_2T$;
2. $(\alpha u_1)T = \alpha(u_1T)$;

for all $u_1, u_2 \in U$, and all $\alpha \in F$.

The Algebra of Linear Transformations

Let V be a vector space over a field F and let Hom (V, V), as before, be the set of all vector-space-homomorphisms of V into itself. In Section 4.3 we showed that Hom (V, V) forms a vector space over F, where, for $T_1, T_2 \in$ Hom (V, V), $T_1 + T_2$ is defined by $v(T_1 + T_2) = vT_1 + vT_2$ for all $v \in V$ and where, for $\alpha \in F$, αT_1 is defined by $v(\alpha T_1) = \alpha(vT_1)$.

For $T_1, T_2 \in$ Hom (V, V), since $vT_1 \in V$ for any $v \in V$, $(vT_1)T_2$ makes sense. As we have done for mappings of any set into itself, we define T_1T_2 by $v(T_1T_2) = (vT_1)T_2$ for any $v \in V$. We now claim that $T_1T_2 \in$ Hom (V, V). To prove this, we must show that for all $\alpha, \beta \in F$ and all $u, v \in V$, $(\alpha u + \beta v)(T_1T_2) = \alpha(u(T_1T_2)) + \beta(v(T_1T_2))$. We compute

$$\begin{aligned}(\alpha u + \beta v)(T_1T_2) &= ((\alpha u + \beta v)T_1)T_2 \\ &= (\alpha(uT_1) + \beta(vT_1))T_2 \\ &= \alpha(uT_1)T_2 + \beta(vT_1)T_2 \\ &= \alpha(u(T_1T_2)) + \beta(v(T_1T_2)).\end{aligned}$$

DEFINITION An associative ring A is called an *algebra* over F if A is a vector space over F such that for all $a, b \in A$ and $\alpha \in F$, $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

DEFINITION A *linear transformation* on V, over F, is an element of $A_F(V)$.

We shall, at times, refer to $A(V)$ as the *ring, or algebra, of linear transformations on V*.

LEMMA 6.1.1 *If A is an algebra, with unit element, over F, then A is isomorphic to a subalgebra of $A(V)$ for some vector space V over F.*

Proof. Since A is an algebra over F, it must be a vector space over F. We shall use $V = A$ to prove the theorem.

If $a \in A$, let $T_a: A \to A$ be defined by $vT_a = va$ for every $v \in A$. We assert that T_a is a linear transformation on $V(=A)$. By the right-distributive law $(v_1 + v_2)T_a = (v_1 + v_2)a = v_1a + v_2a = v_1T_a + v_2T_a$. Since A is an algebra, $(\alpha v)T_a = (\alpha v)a = \alpha(va) = \alpha(vT_a)$ for $v \in A$, $\alpha \in F$. Thus T_a is indeed a linear transformation on A.

Consider the mapping $\psi: A \to A(V)$ defined by $a\psi = T_a$ for every $a \in A$. We claim that ψ is an isomorphism of A into $A(V)$. To begin with, if $a, b \in A$ and $\alpha, \beta \in F$, then for all $v \in A$, $vT_{\alpha a+\beta b} = v(\alpha a + \beta b) = \alpha(va) + \beta(vb)$ [by the left-distributive law and the fact that A is an algebra over F] $= \alpha(vT_a) + \beta(vT_b) = v(\alpha T_a + \beta T_b)$ since both T_a and T_b are linear transformations. In consequence, $T_{\alpha a+\beta b} = \alpha T_a + \beta T_b$, whence ψ is a vector-space homomorphism of A into $A(V)$. Next, we compute, for $a, b \in A$, $vT_{ab} = v(ab) = (va)b = (vT_a)T_b = v(T_aT_b)$ (we have used the associative law of A in this computation), which implies that $T_{ab} = T_aT_b$. In this way, ψ is also a ring-homomorphism of A. So far we have proved that ψ is a homomorphism of A, as an algebra, into $A(V)$. All that remains is to determine the kernel of ψ. Let $a \in A$ be in the kernel of ψ; then $a\psi = 0$, whence $T_a = 0$ and so $vT_a = 0$ for all $v \in V$. Now $V = A$, and A has a unit element, e, hence $eT_a = 0$. However, $0 = eT_a = ea = a$, proving that $a = 0$. The kernel of ψ must therefore merely consist of 0, thus implying that ψ is an isomorphism of A into $A(V)$. This completes the proof of the lemma.

LEMMA 6.1.2 *Let A be an algebra, with unit element, over F, and suppose that A is of dimension m over F. Then every element in A satisfies some nontrivial polynomial in $F[x]$ of degree at most m.*

Proof. Let e be the unit element of A; if $a \in A$, consider the $m + 1$ elements $e, a, a^2, \ldots, a^m$ in A. Since A is m-dimensional over F, by Lemma 4.2.4, $e, a, a^2, \ldots, a^m$, being $m + 1$ in number, must be linearly dependent over F. In other words, there are elements $\alpha_0, \alpha_1, \ldots, \alpha_m$ in F, not all 0, such that $\alpha_0 e + \alpha_1 a + \cdots + \alpha_m a^m = 0$. But then a satisfies the nontrivial polynomial $q(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$, of degree at most m, in $F[x]$.

THEOREM 6.1.1 *If V is an n-dimensional vector space over F, then, given any element T in $A(V)$, there exists a nontrivial polynomial $q(x) \in F[x]$ of degree at most n^2, such that $q(T) = 0$.*

DEFINITION An element $T \in A(V)$ is called *right-invertible* if there exists an $S \in A(V)$ such that $TS = 1$. (Here 1 denotes the unit element of $A(V)$.)

Similarly, we can define left-invertible, if there is a $U \in A(V)$ such that $UT = 1$. If T is both right- and left-invertible and if $TS = UT = 1$, it is an easy exercise that $S = U$ and that S is unique.

DEFINITION An element T in $A(V)$ is *invertible* or *regular* if it is both right- and left-invertible; that is, if there is an element $S \in A(V)$ such that $ST = TS = 1$. We write S as T^{-1}.

THEOREM 6.1.2 *If V is finite-dimensional over F, then $T \in A(V)$ is invertible if and only if the constant term of the minimal polynomial for T is not 0.*

Proof. Let $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_k x^k$, $\alpha_k \neq 0$, be the minimal polynomial for T over F.

If $\alpha_0 \neq 0$, since $0 = p(T) = \alpha_k T^k + \alpha_{k-1} T^{k-1} + \cdots + \alpha_1 T + \alpha_0$, we obtain

$$1 = T\left(-\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \alpha_{k-1} T^{k-2} + \cdots + \alpha_1)\right)$$
$$= \left(-\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \cdots + \alpha_1)\right) T.$$

Therefore,

$$S = -\frac{1}{\alpha_0} (\alpha_k T^{k-1} + \cdots + \alpha_1)$$

acts as an inverse for T, whence T is invertible.

Suppose, on the other hand, that T is invertible, yet $\alpha_0 = 0$. Thus $0 = \alpha_1 T + \alpha_2 T^2 + \cdots + \alpha_k T^k = (\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1})T$. Multiplying this relation from the right by T^{-1} yields $\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1} = 0$, whereby T satisfies the polynomial $q(x) = \alpha_1 + \alpha_2 x + \cdots +$

$\alpha_k x^{k-1}$ in $F[x]$. Since the degree of $q(x)$ is less than that of $p(x)$, this is impossible. Consequently, $\alpha_0 \neq 0$ and the other half of the theorem is established.

COROLLARY 1 *If V is finite-dimensional over F and if $T \in A(V)$ is invertible, then T^{-1} is a polynomial expression in T over F.*

Proof. Since T is invertible, by the theorem, $\alpha_0 + \alpha_1 T + \cdots + \alpha_k T^k = 0$ with $\alpha_0 \neq 0$. But then

$$T^{-1} = -\frac{1}{\alpha_0}(\alpha_1 + \alpha_2 T + \cdots + \alpha_k T^{k-1}).$$

COROLLARY 2 *If V is finite-dimensional over F and if $T \in A(V)$ is singular, then there exists an $S \neq 0$ in $A(V)$ such that $ST = TS = 0$.*

Proof. Because T is not regular, the constant term of its minimal polynomial must be 0. That is, $p(x) = \alpha_1 x + \cdots + \alpha_k x^k$, whence $0 = \alpha_1 T + \cdots + \alpha_k T^k$. If $S = \alpha_1 + \cdots + \alpha_k T^{k-1}$, then $S \neq 0$ (since $\alpha_1 + \cdots + \alpha_k x^{k-1}$ is of lower degree than $p(x)$) and $ST = TS = 0$.

COROLLARY 3 *If V is finite-dimensional over F and if $T \in A(V)$ is right-invertible, then it is invertible.*

Proof. Let $TU = 1$. If T were singular, there would be an $S \neq 0$ such that $ST = 0$. However, $0 = (ST)U = S(TU) = S1 = S \neq 0$, a contradiction. Thus T is regular.

THEOREM 6.1.3 *If V is finite-dimensional over F, then $T \in A(V)$ is singular if and only if there exists a $v \neq 0$ in V such that $vT = 0$.*

Proof. By Corollary 2 to Theorem 6.1.2, T is singular if and only if there is an $S \neq 0$ in $A(V)$ such that $ST = TS = 0$. Since $S \neq 0$ there is an element $w \in V$ such that $wS \neq 0$.

Let $v = wS$; then $vT = (wS)T = w(ST) = w0 = 0$. We have produced a nonzero vector v in V which is annihilated by T. Conversely, if $vT = 0$ with $v \neq 0$, we leave as an exercise the fact that T is not invertible.

DEFINITION If $T \in A(V)$, then the *range* of T, VT, is defined by $VT = \{vT \mid v \in V\}$.

THEOREM 6.1.4 *If V is finite-dimensional over F, then $T \in A(V)$ is regular if and only if T maps V onto V.*

Proof. As happens so often, one-half of this is almost trivial; namely, if T is regular then, given $v \in V$, $v = (vT^{-1})T$, whence $VT = V$ and T is onto.

On the other hand, suppose that T is not regular. We must show that T is not onto. Since T is singular, by Theorem 6.1.3, there exists a vector $v_1 \neq 0$ in V such that $v_1 T = 0$. By Lemma 4.2.5 we can fill out, from v_1, to a basis $v_1, v_2, \ldots, v_n$ of V. Then every element in VT is a linear combination of the elements $w_1 = v_1 T$, $w_2 = v_2 T, \ldots, w_n = v_n T$. Since $w_1 = 0$, VT is spanned by the $n - 1$ elements $w_2, \ldots, w_n$; therefore $\dim VT \leq n - 1 < n = \dim V$. But then VT must be different from V; that is, T is not onto.

DEFINITION If V is finite-dimensional over F, then the *rank* of T is the dimension of VT, the range of T, over F.

We denote the rank of T by $r(T)$. At one end of the spectrum, if $r(T) = \dim V$, T is regular (and so, not at all singular). At the other end, if $r(T) = 0$, then $T = 0$ and so T is as singular as it can possibly be. The rank, as a function on $A(V)$, is an important function, and we now investigate some of its properties.

LEMMA 6.1.3 *If V is finite-dimensional over F then for $S, T \in A(V)$.*

1. $r(ST) \leq r(T)$;
2. $r(TS) \leq r(T)$;

(and so, $r(ST) \leq \min\{r(T), r(S)\}$*)*

3. $r(ST) = r(TS) = r(T)$ *for S regular in $A(V)$.*

Proof. We go through 1, 2, and 3 in order.

1. Since $VS \subset V$, $V(ST) = (VS)T \subset VT$, whence, by Lemma 4.2.6, $\dim(V(ST)) \leq \dim VT$; that is, $r(ST) \leq r(T)$.

2. Suppose that $r(T) = m$. Therefore, VT has a basis of m elements, $w_1, w_2, \ldots, w_m$. But then $(VT)S$ is spanned by $w_1 S, w_2 S, \ldots, w_m S$, hence has dimension at most m. Since $r(TS) = \dim(V(TS)) = \dim((VT)S) \leq m = \dim VT = r(T)$, part 2 is proved.

3. If S is invertible then $VS = V$, whence $V(ST) = (VS)T = VT$. Thereby, $r(ST) = \dim(V(ST)) = \dim(VT) = r(T)$. On the other hand, if VT has $w_1, \ldots, w_m$ as a basis, the regularity of S implies that $w_1S, \ldots, w_mS$ are linearly independent. (Prove!) Since these span $V(TS)$ they form a basis of $V(TS)$. But then $r(TS) = \dim(V(TS)) = \dim(VT) = r(T)$.

COROLLARY *If $T \in A(V)$ and if $S \in A(V)$ is regular, then $r(T) = r(STS^{-1})$.*

Proof. By part 3 of the lemma, $r(STS^{-1}) = r(S(TS^{-1})) = r((TS^{-1})S) = r(T)$.

MATRIX REPRESENTATION ON LINEAR TRANSFORMATION

Let V be an n-dimensional vector space over a field F and let $v_1, \ldots, v_n$ be a basis of V over F. If $T \in A(V)$ then T is determined on any vector as soon as we know its action on a basis of V. Since T maps V into V, v_1T, $v_2T, \ldots, v_nT$ must all be in V. As elements of V, each of these is realizable in a *unique* way as a linear combination of $v_1, \ldots, v_n$ over F. Thus

$$\begin{aligned}
v_1T &= \alpha_{11}v_1 + \alpha_{12}v_2 + \cdots + \alpha_{1n}v_n \\
v_2T &= \alpha_{21}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{2n}v_n \\
v_iT &= \alpha_{i1}v_1 + \alpha_{i2}v_2 + \cdots + \alpha_{in}v_n \\
&\vdots \\
v_nT &= \alpha_{n1}v_1 + \alpha_{n2}v_2 + \cdots + \alpha_{nn}v_n,
\end{aligned}$$

where each $\alpha_{ij} \in F$. This system of equations can be written more compactly as

$$v_iT = \sum_{j=1}^{n} \alpha_{ij}v_j, \qquad \text{for} \quad i = 1, 2, \ldots, n.$$

The ordered set of n^2 numbers α_{ij} in F completely describes T. They will serve as the means of representing T.

DEFINITION Let V be an n-dimensioned vector space over F and let $v_1, \ldots, v_n$ be a basis for V over F. If $T \in A(V)$ then the *matrix of T in the basis $v_1, \ldots, v_n$*, written as $m(T)$, is

$$m(T) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix},$$

where $v_iT = \sum_j \alpha_{ij}v_j$.

A matrix then is an ordered, square array of elements of F, with, as yet, no further properties, which represents the effect of a linear transformation on a given basis.

Let us examine an example. Let F be a field and let V be the set of all polynomials in x of degree $n-1$ or less over F. On V let D be defined by $(\beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1})D = \beta_1 + 2\beta_2 x + \cdots + i\beta_i x^{i-1} + \cdots + (n-1)\beta_{n-1}x^{n-2}$. It is trivial that D is a linear transformation on V; in fact, it is merely the differentiation operator.

What is the matrix of D? The questions is meaningless unless we specify a basis of V. Let us first compute the matrix of D in the basis $v_1 = 1$, $v_2 = x$, $v_3 = x^2, \ldots, v_i = x^{i-1}, \ldots, v_n = x^{n-1}$. Now,

$$\begin{aligned}
v_1 D &= 1D = 0 = 0v_1 + 0v_2 + \cdots + 0v_n \\
v_2 D &= xD = 1 = 1v_1 + 0v_2 + \cdots + 0v_n \\
&\vdots \\
v_i D &= x^{i-1}D = (i-1)x^{i-2} \\
&= 0v_1 + 0v_2 + \cdots + 0v_{i-2} + (i-1)v_{i-1} + 0v_i \\
&\quad + \cdots + 0v_n \\
&\vdots \\
v_n D &= x^{n-1}D = (n-1)x^{n-2} \\
&= 0v_1 + 0v_2 + \cdots + 0v_{n-2} + (n-1)v_{n-1} + 0v_n.
\end{aligned}$$

Going back to the very definition of the matrix of a linear transformation in a given basis, we see the matrix of D in the basis $v_1, \ldots, v_n$, $m_1(D)$, is in fact

$$m_1(D) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 3 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & (n-1) & 0 \end{pmatrix}$$

THEOREM 6.3.1 *The set of all $n \times n$ matrices over F form an associative algebra, F_n, over F. If V is an n-dimensional vector space over F, then $A(V)$ and F_n are isomorphic as algebras over F. Given any basis $v_1, \ldots, v_n$ of V over F, if for $T \in A(V)$, $m(T)$ is the matrix of T in the basis $v_1, \ldots. v_n$, the mapping $T \to m(T)$ provides an algebra isomorphism of $A(V)$ onto F_n.*

The zero under addition in F_n is the *zero-matrix* all of whose entries are 0; we shall often write it merely as 0. The *unit matrix*, which is the unit element of F_n under multiplication, is the matrix whose diagonal entries are 1 and whose entries elsewhere are 0; we shall write it as I, I_n (when we wish to emphasize the size of matrices), or merely as 1. For $\alpha \in F$, the matrices

$$\alpha I = \begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix}$$

(*blank spaces indicate only* 0 *entries*) are called *scalar matrices*. Because of the isomorphism between $A(V)$ and F_n, it is clear that $T \in A(V)$ is invertible if and only if $m(T)$, as a matrix, has an inverse in F_n.

THEOREM 6.3.2 *If V is n-dimensional over F and if $T \in A(V)$ has the matrix $m_1(T)$ in the basis $v_1, \ldots, v_n$ and the matrix $m_2(T)$ in the basis $w_1, \ldots, w_n$ of V over F, then there is an element $C \in F_n$ such that $m_2(T) = Cm_1(T)C^{-1}$.*

In fact, if S is the linear transformation of V defined by $v_iS = w_i$ for $i = 1, 2, \ldots, n$, then C can be chosen to be $m_1(S)$.

Proof. Let $m_1(T) = (\alpha_{ij})$ and $m_2(T) = (\beta_{ij})$; thus $v_iT = \sum_j \alpha_{ij}v_j$, $w_iT = \sum_j \beta_{ij}w_j$.

Let S be the linear transformation on V defined by $v_iS = w_i$. Since $v_1, \ldots, v_n$ and $w_1, \ldots, w_n$ are bases of V over F, S maps V onto V, hence, by Theorem 6.1.4, S is invertible in $A(V)$.

Now $w_iT = \sum_j \beta_{ij}w_j$; since $w_i = v_iS$, on substituting this in the expression for w_iT we obtain $(v_iS)T = \sum_j \beta_{ij}(v_jS)$. But then $v_i(ST) = (\sum_j \beta_{ij}v_j)S$; since S is invertible, this further simplifies to $v_i(STS^{-1}) = \sum_j \beta_{ij}v_j$. By the very definition of the matrix of a linear transformation in a given basis, $m_1(STS^{-1}) = (\beta_{ij}) = m_2(T)$. However, the mapping $T \to m_1(T)$ is an isomorphism of $A(V)$ onto F_n; therefore, $m_1(STS^{-1}) = m_1(S)m_1(T)m_1(S^{-1}) = m_1(S)m_1(T)m_1(S)^{-1}$. Putting the pieces together, we obtain $m_2(T) = m_1(S)m_1(T)m_1(S)^{-1}$, which is exactly what is claimed in the theorem.

UNIT-III

SYLLABUS

Isomorphism theorems -Invertability and isomorphisms - change of coordinate matrix.

THE ISOMORPHISM THEOREMS

Definition 1. *Let $R = (R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings. A set map $\phi\colon R \to S$ is a (ring) homomorphism if*

(1) $\phi(r_1 +_R r_2) = \phi(r_1) +_S \phi(r_2)$ *for all* $r_1, r_2 \in R$,
(2) $\phi(r_1 \cdot_R r_2) = \phi(r_1) \cdot_S \phi(r_2)$ *for all* $r_1, r_2 \in R$, *and*
(3) $\phi(1_R) = 1_S$.

For simplicity, we will often write conditions (1) and (2) as $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ with the particular addition and multiplication implicit.

Remark 1. *If $\phi\colon (R, +, \cdot) \to (S, +, \cdot)$ is a ring homomorphism then $\phi\colon (R, +) \to (S, +)$ is a group homomorphism.*

Example 1. *If R is any ring and $S \subset R$ is a subring, then the inclusion $i\colon S \hookrightarrow R$ is a ring homomorphism.*

Exercise 1. *Prove that*

$$\varphi\colon \mathbb{Q} \to \mathrm{M}_n(\mathbb{Q}), \quad \varphi(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

is a ring homomorphism.

Lemma 1. *Let $\phi\colon R \to S$ be a ring homomorphism. Then*

(1) $\phi(0_R) = 0_S$,
(2) $\phi(-r) = -\phi(r)$ *for all* $r \in R$,
(3) *if* $r \in R^\times$ *then* $\phi(r) \in S^\times$ *and* $\phi(r^{-1}) = \phi(r)^{-1}$, *and*
(4) *if* $R' \subset R$ *is a subring, then* $\phi(R')$ *is a subring of* S.

Proof. Statements (1) and (2) hold because of Remark 1. We will repeat the proofs here for the sake of completeness.

Since $0_R + 0_R = 0_R$, $\phi(0_R) + \phi(0_R) = \phi(0_R)$. Then since S is a ring, $\phi(0_R)$ has an additive inverse, which we may add to both sides. Thus we obtain

$$\phi(0_R) = \phi(0_R) + \phi(0_R) + -\phi(0_R) = \phi(0_R) + -\phi(0_R) = 0_S,$$

as desired.

Let $r \in R$. Since $r + -r = -r + r = 0_R$, we have

$$\phi(r) + \phi(-r) = \phi(-r) + \phi(r) = \phi(0_R) = 0_S,$$

where the last equality comes from (1). Thus $\phi(-r) = -\phi(r)$ as additive inverses are unique.

Now let $r \in R^\times$. Then there exists $r^{-1} \in R$ such that $r \cdot r^{-1} = r^{-1} \cdot r = 1_R$. Then since ϕ is a ring homomorphism we have

$$\phi(r) \cdot \phi(r^{-1}) = \phi(r^{-1})\phi(r) = \phi(1_R) = 1_S.$$

Thus $\phi(r)$ has a multiplicative inverse and it is $\phi(r^{-1})$.

Lastly, let $R' \subset R$ be a subring. To show that $\phi(R')$ is a subring we must show that $1_S \in \phi(R')$ and for all $s_1, s_2 \in \phi(R')$, $s_1 - s_2$ and $s_1 s_2$ are also in $\phi(R')$. Since $s_1, s_2 \in \phi(R')$, there exists $r_1, r_2 \in R'$ such that $\phi(r_1) = s_1$ and $\phi(r_2) = s_2$. Thus

$$s_1 - s_2 = \phi(r_1) - \phi(r_2) = \phi(r_1) + \phi(-r_2) = \phi(r_1 - r_2), \quad \text{and} \quad s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2).$$

Since R' is a subring, $r_1 - r_2$ and $r_1 r_2$ are contained in R'. Hence $s_1 - s_2$ and $s_1 s_2$ are in $\phi(R')$. Furthermore, $1_R \in R'$ so $1_S = \phi(1_R) \in \phi(R')$. Therefore, $\phi(R')$ is a subring of S. ☐

Definition 2. *Let R and S be rings and let $\phi\colon R \to S$ be a set map. We say that ϕ is a (ring) isomorphism if*

(1) *ϕ is a (ring) homomorphism and*
(2) *ϕ is a bijection on sets.*

We say that two rings R_1 and R_2 are isomorphic if there exists an isomorphism between them.

Lemma 2. *Let R and S be rings and let $\phi\colon R \to S$ be an isomorphism. Then:*

(1) *ϕ^{-1} is an isomorphism,*
(2) *$r \in R$ is a unit if and only if $\phi(r)$ is a unit of S,*
(3) *$r \in R$ is a zero divisor if and only if $\phi(r)$ is a zero divisor of S,*
(4) *R is commutative if and only if S is commutative,*
(5) *R is an integral domain if and only if S is an integral domain, and*
(6) *R is a field if and only if S is a field.*

Kernel, image, and the isomorphism theorems

Definition 3. *Let $\phi\colon R \to S$ be a ring homomorphism. The kernel of ϕ is*

$$\ker\phi := \{r \in R : \phi(r) = 0\} \subset R$$

and the image of ϕ is

$$\operatorname{im}\phi := \{s \in S : s = \phi(r) \text{ for some } r \in R\} \subset S.$$

Theorem 3 (First isomorphism theorem). *Let R and S be rings and let $\phi\colon R \to S$ be a homomorphism. Then:*

(1) *The kernel of ϕ is an ideal of R,*
(2) *The image of ϕ is a subring of S,*
(3) *The map*

$$\varphi\colon R/\ker\phi \to \operatorname{im}\phi \subset S, \quad r + \ker\phi \mapsto \phi(r)$$

is a well-defined isomorphism.

Proof. The image of ϕ is a subring by Lemma 1. Let us prove that $\ker\phi$ is an ideal. By Lemma 1, $\phi(0) = 0$ so $0 \in \ker\phi$ and hence the kernel is nonempty. Let $a, b \in \ker\phi$ and let $r \in R$. Then since ϕ is a homomorphism we have

$$\begin{aligned}\phi(a+b) &= \phi(a)+\phi(b) = 0+0 = 0,\\ \phi(ra) &= \phi(r)\phi(a) = \phi(r)\cdot 0 = 0,\\ \phi(ar) &= \phi(a)\phi(r) = 0\cdot\phi(r) = 0.\end{aligned}$$

Thus $a+b, ra$, and ar are in $\ker\phi$ and so $\ker\phi$ is an ideal.

Consider the map φ. We first show that it is well-defined. Let $r, r' \in R$ be such that $r - r' \in \ker\phi$, i.e., such that $r + \ker\phi = r' + \ker\phi$. Then

$$\phi(r) = \phi(r' + (r - r')) = \phi(r') + \phi(r - r') = \phi(r') + 0 = \phi(r'),$$

so φ is well defined. Let $r_1 + I, r_2 + I \in R/I$. Then since ϕ is a homomorphism we have:

$$\begin{aligned}\varphi(r_1+I+r_2+I) &= \varphi(r_1+r_2+I) = \phi(r_1+r_2) = \phi(r_1)+\phi(r_2)\\ &= \varphi(r_1+I)+\varphi(r_2+I)\\ \varphi((r_1+I)(r_2+I)) &= \varphi(r_1r_2+I) = \phi(r_1r_2) = \phi(r_1)\phi(r_2)\\ &= \varphi(r_1+I)\varphi(r_2+I)\\ \varphi(1+I) &= \phi(1) = 1.\end{aligned}$$

Therefore φ is a homomorphism.

Let us prove that φ is bijective. If $r + \ker\phi \in \ker\varphi$, then $\varphi(r+I) = \phi(r) = 0$ and so $r \in \ker\phi$ or equivalently $r + \ker\phi = \ker\phi$. Thus $\ker\varphi$ is trivial and so by Exercise 9, φ is injective. Let $s \in \operatorname{im}\phi$. Then there exists an $r \in R$ such that $\phi(r) = s$ or equivalently that $\varphi(r + \ker\phi) = s$. Thus $s \in \operatorname{im}\varphi$ and so φ is surjective. Hence φ is an isomorphism as desired. □

Theorem 4 (Second isomorphism theorem). *Let R be a ring, let $S \subset R$ be a subring, and let I be an ideal of R. Then:*

(1) *$S + I := \{s + a : s \in S, a \in I\}$ is a subring of R,*
(2) *$S \cap I$ is an ideal of S, and*
(3) *$(S+I)/I$ is isomorphic to $S/(S\cap I)$.*

Proof. **(1)**: S is a subring and I is an ideal so $1 + 0 \in S + I$. Let $s_1 + a_1$ and $s_2 + a_2$ be elements of $S + I$. Then

$$(s_1+a_1)-(s_2+a_2) = \underbrace{(s_1-s_2)}_{\in S} + \underbrace{(a_1-a_2)}_{\in I} \quad \text{and} \quad (s_1+a_1)(s_2+a_2) = \underbrace{s_1s_2}_{\in S} + \underbrace{s_1a_2+a_1s_2+a_1a_2}_{\in I}$$

Hence $S + I$ is a subring of R.

(2): The intersection $S \cap I$ is nonempty since 0 is contained in I and S. Let $a_1, a_2 \in S \cap I$ and let $s \in S$. Then $a_1 + a_2 \in S \cap I$ since S and I are both closed under addition. Furthermore sa_1 and a_1s are in $S \cap I$ since I is closed under multiplication from $R \supset S$ and S is closed under multiplication. Therefore $S \cap I$ is an ideal of S.

(3): Consider the map $\phi\colon S \to (S+I)/I$ which sends an element s to $s+I$. This is a ring homomorphism by definition of addition and multiplication in quotient rings. We claim that it is surjective with kernel $S \cap I$, which would complete the proof by the first isomorphism theorem. Consider elements $s \in S$ and $a \in I$. Then $s + a + I = s + I$ since $a \in I$, so $s + a + I \in \operatorname{im}\phi$ and hence ϕ is surjective. Let $s \in S$ be an element of $\ker\phi$. Then $s + I = I$ which holds if and only if $s \in I$ or equivalently if $s \in S \cap I$. Thus $\ker\phi = S \cap I$ and we have our desired result. □

Theorem 5 (Third isomorphism theorem). *Let R be a ring and let $J \subset I$ be ideals of R. Then I/J is an ideal of R/J and*

$$\frac{R/J}{I/J} \cong R/I.$$

Proof. Since I and J are ideals, they are nonempty and so $I/J = \{a + J : a \in I\}$ is also nonempty. Let $a_1, a_2 \in I$ and let $r \in R$. By definition of addition and multiplication of cosets, we have

$$(a_1 + J) + (a_2 + J) = (a_1 + a_2) + J,$$
$$(r + J)(a_1 + J) = ra_1 + J, \text{ and}$$
$$(a_1 + J)(r + J) = a_1 r + J.$$

Since I is an ideal, $a_1 + a_2, ra_1$, and $a_1 r$ are contained in I so I/J is an ideal of R/J.

Consider the map $\phi\colon R/J \to R/I$ that sends $r + J$ to $r + I$. We claim that this is a well-defined surjective homomorphism with kernel equal to I/J. (See Exercise 11.) Then $(R/J)/(I/J)$ is isomorphic to R/I by the first isomorphism theorem. □

Matrix Representation of a Linear Operator

Let T be a linear operator (transformation) from a vector space V into itself, and suppose $S = \{u_1, u_2, \ldots, u_n\}$ is a basis of V. Now $T(u_1), T(u_2), \ldots, T(u_n)$ are vectors in V, and so each is a linear combination of the vectors in the basis S; say,

$$\begin{aligned} T(u_1) &= a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n \\ T(u_2) &= a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ T(u_n) &= a_{n1}u_1 + a_{n2}u_2 + \cdots + a_{nn}u_n \end{aligned}$$

The following definition applies.

DEFINITION: The transpose of the above matrix of coefficients, denoted by $m_S(T)$ or $[T]_S$, is called the *matrix representation* of T relative to the basis S, or simply the matrix of T in the basis S. (The subscript S may be omitted if the basis S is understood.)

Using the coordinate (column) vector notation, the matrix representation of T may be written in the form

$$m_S(T) = [T]_S = \left[[T(u_1)]_S,\ [T(u_2)]_S,\ \ldots,\ [T(u_1)]_S\right]$$

That is, the columns of $m(T)$ are the coordinate vectors of $T(u_1), T(u_2), \ldots, T(u_n)$, respectively.

EXAMPLE 6.1 Let $F: \mathbf{R}^2 \to \mathbf{R}^2$ be the linear operator defined by $F(x, y) = (2x + 3y,\ 4x - 5y)$.

(a) Find the matrix representation of F relative to the basis $S = \{u_1, u_2\} = \{(1, 2),\ (2, 5)\}$.

(1) First find $F(u_1)$, and then write it as a linear combination of the basis vectors u_1 and u_2. (For notational convenience, we use column vectors.) We have

$$F(u_1) = F\left(\begin{bmatrix}1\\2\end{bmatrix}\right) = \begin{bmatrix}8\\-6\end{bmatrix} = x\begin{bmatrix}1\\2\end{bmatrix} + y\begin{bmatrix}2\\5\end{bmatrix} \quad \text{and} \quad \begin{aligned} x + 2y &= 8 \\ 2x + 5y &= -6 \end{aligned}$$

Solve the system to obtain $x = 52$, $y = -22$. Hence, $F(u_1) = 52u_1 - 22u_2$.

(2) Next find $F(u_2)$, and then write it as a linear combination of u_1 and u_2:

$$F(u_2) = F\left(\begin{bmatrix}2\\5\end{bmatrix}\right) = \begin{bmatrix}19\\-17\end{bmatrix} = x\begin{bmatrix}1\\2\end{bmatrix} + y\begin{bmatrix}2\\5\end{bmatrix} \quad \text{and} \quad \begin{aligned} x + 2y &= 19 \\ 2x + 5y &= -17 \end{aligned}$$

Solve the system to get $x = 129$, $y = -55$. Thus, $F(u_2) = 129u_1 - 55u_2$.

Now write the coordinates of $F(u_1)$ and $F(u_2)$ as columns to obtain the matrix

$$[F]_S = \begin{bmatrix} 52 & 129 \\ -22 & -55 \end{bmatrix}$$

(b) Find the matrix representation of F relative to the (usual) basis $E = \{e_1, e_2\} = \{(1, 0),\ (0, 1)\}$.

Find $F(e_1)$ and write it as a linear combination of the usual basis vectors e_1 and e_2, and then find $F(e_2)$ and write it as a linear combination of e_1 and e_2. We have

$$\begin{aligned} F(e_1) &= F(1, 0) = (2, 2) \quad = 2e_1 + 4e_2 \\ F(e_2) &= F(0, 1) = (3, -5) = 3e_1 - 5e_2 \end{aligned} \quad \text{and so} \quad [F]_E = \begin{bmatrix} 2 & 3 \\ 4 & -5 \end{bmatrix}$$

Note that the coordinates of $F(e_1)$ and $F(e_2)$ form the columns, not the rows, of $[F]_E$. Also, note that the arithmetic is much simpler using the usual basis of $\mathbf{R}^2$.

EXAMPLE 6.2 Let V be the vector space of functions with basis $S = \{\sin t, \cos t, e^{3t}\}$, and let $\mathbf{D}: V \to V$ be the differential operator defined by $\mathbf{D}(f(t)) = d(f(t))/dt$. We compute the matrix representing $\mathbf{D}$ in the basis S:

$$\begin{aligned} \mathbf{D}(\sin t) &= \quad \cos t = \quad 0(\sin t) + 1(\cos t) + 0(e^3 t) \\ \mathbf{D}(\cos\ t) &= -\sin t = -1(\sin t) + 0(\cos t) + 0(e^{3t}) \\ \mathbf{D}(e^{3t}) &= \quad 3e^{3t} = \quad 0(\sin t) + 0(\cos t) + 3(e^{3t}) \end{aligned}$$

and so

$$[\mathbf{D}] = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

Note that the coordinates of $\mathbf{D}(\sin t)$, $\mathbf{D}(\cos t)$, $\mathbf{D}(e^{3t})$ form the columns, not the rows, of $[\mathbf{D}]$.

Matrix Mappings and Their Matrix Representation

Consider the following matrix A, which may be viewed as a linear operator on $\mathbf{R}^2$, and basis S of $\mathbf{R}^2$:

$$A = \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix} \quad \text{and} \quad S = \{u_1, u_2\} = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 5 \end{bmatrix} \right\}$$

(We write vectors as columns, because our map is a matrix.) We find the matrix representation of A relative to the basis S.

(1) First we write $A(u_1)$ as a linear combination of u_1 and u_2. We have

$$A(u_1) = \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} -1 \\ -6 \end{bmatrix} = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} 2 \\ 5 \end{bmatrix} \quad \text{and so} \quad \begin{aligned} x + 2y &= -1 \\ 2x + 5y &= -6 \end{aligned}$$

Solving the system yields $x = 7$, $y = -4$. Thus, $A(u_1) = 7u_1 - 4u_2$.

(2) Next we write $A(u_2)$ as a linear combination of u_1 and u_2. We have

$$A(u_2) = \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix}\begin{bmatrix} 2 \\ 5 \end{bmatrix} = \begin{bmatrix} -4 \\ -7 \end{bmatrix} = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} 2 \\ 5 \end{bmatrix} \quad \text{and so} \quad \begin{aligned} x + 2y &= -4 \\ 2x + 5y &= -7 \end{aligned}$$

Solving the system yields $x = -6$, $y = 1$. Thus, $A(u_2) = -6u_1 + u_2$. Writing the coordinates of $A(u_1)$ and $A(u_2)$ as columns gives us the following matrix representation of A:

$$[A]_S = \begin{bmatrix} 7 & -6 \\ -4 & 1 \end{bmatrix}$$

Remark: Suppose we want to find the matrix representation of A relative to the usual basis $E = \{e_1, e_2\} = \{[1, 0]^T, \ [0, 1]^T\}$ of $\mathbf{R}^2$. We have

$$\begin{aligned} A(e_1) &= \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = 3e_1 + 4e_2 \\ A(e_2) &= \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -2 \\ -5 \end{bmatrix} = -2e_1 - 5e_2 \end{aligned} \quad \text{and so} \quad [A]_E = \begin{bmatrix} 3 & -2 \\ 4 & -5 \end{bmatrix}$$

Note that $[A]_E$ is the original matrix A. This result is true in general:

> The matrix representation of any $n \times n$ square matrix A over a field K relative to the usual basis E of K^n is the matrix A itself; that is,
> $$[A]_E = A$$

Algorithm for Finding Matrix Representations

Next follows an algorithm for finding matrix representations. The first Step 0 is optional. It may be useful to use it in Step 1(b), which is repeated for each basis vector.

ALGORITHM 6.1: The input is a linear operator T on a vector space V and a basis $S = \{u_1, u_2, \ldots, u_n\}$ of V. The output is the matrix representation $[T]_S$.

Step 0. Find a formula for the coordinates of an arbitrary vector v relative to the basis S.

Step 1. Repeat for each basis vector u_k in S:

(a) Find $T(u_k)$.

(b) Write $T(u_k)$ as a linear combination of the basis vectors $u_1, u_2, \dots, u_n$.

Step 2. Form the matrix $[T]_S$ whose columns are the coordinate vectors in Step 1(b).

EXAMPLE 6.3 Let $F: \mathbf{R}^2 \to \mathbf{R}^2$ be defined by $F(x, y) = (2x + 3y,\ 4x - 5y)$. Find the matrix representation $[F]_S$ of F relative to the basis $S = \{u_1, u_2\} = \{(1, -2),\ (2, -5)\}$.

(Step 0) First find the coordinates of $(a, b) \in \mathbf{R}^2$ relative to the basis S. We have

$$\begin{bmatrix} a \\ b \end{bmatrix} = x\begin{bmatrix} 1 \\ -2 \end{bmatrix} + y\begin{bmatrix} 2 \\ -5 \end{bmatrix} \quad \text{or} \quad \begin{aligned} x + 2y &= a \\ -2x - 5y &= b \end{aligned} \quad \text{or} \quad \begin{aligned} x + 2y &= a \\ -y &= 2a + b \end{aligned}$$

Solving for x and y in terms of a and b yields $x = 5a + 2b$, $y = -2a - b$. Thus,

$$(a, b) = (5a + 2b)u_1 + (-2a - b)u_2$$

(Step 1) Now we find $F(u_1)$ and write it as a linear combination of u_1 and u_2 using the above formula for (a, b), and then we repeat the process for $F(u_2)$. We have

$$\begin{aligned} F(u_1) &= F(1, -2) = \ \ (-4, 14) = 8u_1 - 6u_2 \\ F(u_2) &= F(2, -5) = (-11, 33) = 11u_1 - 11u_2 \end{aligned}$$

(Step 2) Finally, we write the coordinates of $F(u_1)$ and $F(u_2)$ as columns to obtain the required matrix:

$$[F]_S = \begin{bmatrix} 8 & 11 \\ -6 & -11 \end{bmatrix}$$

Properties of Matrix Representations

This subsection gives the main properties of the matrix representations of linear operators T on a vector space V. We emphasize that we are always given a particular basis S of V.

Our first theorem, proved in Problem 6.9, tells us that the ''action'' of a linear operator T on a vector v is preserved by its matrix representation.

THEOREM 6.1: Let $T: V \to V$ be a linear operator, and let S be a (finite) basis of V. Then, for any vector v in V, $[T]_S[v]_S = [T(v)]_S$.

EXAMPLE 6.4 Consider the linear operator F on R^2 and the basis S of Example 6.3; that is,

$$F(x, y) = (2x + 3y, \quad 4x - 5y) \qquad \text{and} \qquad S = \{u_1, u_2\} = \{(1, -2), \quad (2, -5)\}$$

Let

$$v = (5, -7), \qquad \text{and so} \qquad F(v) = (-11, 55)$$

Using the formula from Example 6.3, we get

$$[v] = [11, -3]^T \qquad \text{and} \qquad [F(v)] = [55, -33]^T$$

We verify Theorem 6.1 for this vector v (where $[F]$ is obtained from Example 6.3):

$$[F][v] = \begin{bmatrix} 8 & 11 \\ -6 & -11 \end{bmatrix} \begin{bmatrix} 11 \\ -3 \end{bmatrix} = \begin{bmatrix} 55 \\ -33 \end{bmatrix} = [F(v)]$$

THEOREM 6.2: Let V be an n-dimensional vector space over K, let S be a basis of V, and let $\mathbf{M}$ be the algebra of $n \times n$ matrices over K. Then the mapping

$$m: A(V) \to \mathbf{M} \qquad \text{defined by} \qquad m(T) = [T]_S$$

is a vector space isomorphism. That is, for any $F, G \in A(V)$ and any $k \in K$,

(i) $m(F+G) = m(F) + m(G)$ or $[F+G] = [F] + [G]$
(ii) $m(kF) = km(F)$ or $[kF] = k[F]$
(iii) m is bijective (one-to-one and onto).

Change of Basis

Let V be an n-dimensional vector space over a field K. We have shown that once we have selected a basis S of V, every vector $v \in V$ can be represented by means of an n-tuple $[v]_S$ in K^n, and every linear operator T in $A(V)$ can be represented by an $n \times n$ matrix over K. We ask the following natural question:

How do our representations change if we select another basis?

In order to answer this question, we first need a definition.

DEFINITION: Let $S = \{u_1, u_2, \ldots, u_n\}$ be a basis of a vector space V, and let $S' = \{v_1, v_2, \ldots, v_n\}$ be another basis. (For reference, we will call S the ''old'' basis and S' the ''new'' basis.) Because S is a basis, each vector in the ''new'' basis S' can be written uniquely as a linear combination of the vectors in S; say,

$$\begin{aligned} v_1 &= a_{11}u_1 + a_{12}u_2 + \cdots + a_{1n}u_n \\ v_2 &= a_{21}u_1 + a_{22}u_2 + \cdots + a_{2n}u_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ v_n &= a_{n1}u_1 + a_{n2}u_2 + \cdots + a_{nn}u_n \end{aligned}$$

Let P be the transpose of the above matrix of coefficients; that is, let $P = [p_{ij}]$, where $p_{ij} = a_{ji}$. Then P is called the *change-of-basis matrix* (or *transition matrix*) from the ''old'' basis S to the ''new'' basis S'.

Remark 1: The above change-of-basis matrix P may also be viewed as the matrix whose columns are, respectively, the coordinate column vectors of the ''new'' basis vectors v_i relative to the ''old'' basis S; namely,

$$P = \big[[v_1]_S, [v_2]_S, \ldots, [v_n]_S\big]$$

Remark 2: Analogously, there is a change-of-basis matrix Q from the ''new'' basis S' to the ''old'' basis S. Similarly, Q may be viewed as the matrix whose columns are, respectively, the coordinate column vectors of the ''old'' basis vectors u_i relative to the ''new'' basis S'; namely,

$$Q = \big[[u_1]_{S'}, [u_2]_{S'}, \ldots, [u_n]_{S'}\big]$$

PROPOSITION 6.4: Let P and Q be the above change-of-basis matrices. Then $Q = P^{-1}$.

Now suppose $S = \{u_1, u_2, \ldots, u_n\}$ is a basis of a vector space V, and suppose $P = [p_{ij}]$ is any nonsingular matrix. Then the n vectors

$$v_i = p_{1i}u_i + p_{2i}u_2 + \cdots + p_{ni}u_n, \qquad i = 1, 2, \ldots, n$$

corresponding to the columns of P, are linearly independent [Problem 6.21(a)]. Thus, they form another basis S' of V. Moreover, P will be the change-of-basis matrix from S to the new basis S'.

EXAMPLE 6.5 Consider the following two bases of $\mathbf{R}^2$:

$$S = \{u_1, u_2\} = \{(1, 2),\ (3, 5)\} \qquad \text{and} \qquad S' = \{v_1, v_2\} = \{(1, -1),\ (1, -2)\}$$

(a) Find the change-of-basis matrix P from S to the ''new'' basis S'.

Write each of the new basis vectors of S' as a linear combination of the original basis vectors u_1 and u_2 of S. We have

$$\begin{bmatrix} 1 \\ -1 \end{bmatrix} = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} 3 \\ 5 \end{bmatrix} \quad \text{or} \quad \begin{matrix} x + 3y = 1 \\ 2x + 5y = -1 \end{matrix} \quad \text{yielding} \quad x = -8, \quad y = 3$$

$$\begin{bmatrix} 1 \\ -1 \end{bmatrix} = x\begin{bmatrix} 1 \\ 2 \end{bmatrix} + y\begin{bmatrix} 3 \\ 5 \end{bmatrix} \quad \text{or} \quad \begin{matrix} x + 3y = 1 \\ 2x + 5y = -1 \end{matrix} \quad \text{yielding} \quad x = -11, \quad y = 4$$

Thus,

$$\begin{aligned} v_1 &= -8u_1 + 3u_2 \\ v_2 &= -11u_1 + 4u_2 \end{aligned} \qquad \text{and hence,} \qquad P = \begin{bmatrix} -8 & -11 \\ 3 & 4 \end{bmatrix}.$$

Note that the coordinates of v_1 and v_2 are the columns, not rows, of the change-of-basis matrix P.

(b) Find the change-of-basis matrix Q from the ''new'' basis S' back to the ''old'' basis S.

Here we write each of the ''old'' basis vectors u_1 and u_2 of S' as a linear combination of the ''new'' basis vectors v_1 and v_2 of S'. This yields

$$\begin{aligned} u_1 &= 4v_1 - 3v_2 \\ u_2 &= 11v_1 - 8v_2 \end{aligned} \qquad \text{and hence,} \qquad Q = \begin{bmatrix} 4 & 11 \\ -3 & -8 \end{bmatrix}$$

As expected from Proposition 6.4, $Q = P^{-1}$. (In fact, we could have obtained Q by simply finding P^{-1}.)

EXAMPLE 6.6 Consider the following two bases of $\mathbf{R}^3$:

$$E = \{e_1, e_2, e_3\} = \{(1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1)\}$$

and

$$S = \{u_1, u_2, u_3\} = \{(1, 0, 1), \quad (2, 1, 2), \quad (1, 2, 2)\}$$

(a) Find the change-of-basis matrix P from the basis E to the basis S.

Because E is the usual basis, we can immediately write each basis element of S as a linear combination of the basis elements of E. Specifically,

$$\begin{aligned} u_1 &= (1, 0, 1) = e_1 + e_3 \\ u_2 &= (2, 1, 2) = 2e_1 + e_2 + 2e_3 \\ u_3 &= (1, 2, 2) = e_1 + 2e_2 + 2e_3 \end{aligned} \qquad \text{and hence,} \qquad P = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 2 \end{bmatrix}$$

Again, the coordinates of u_1, u_2, u_3 appear as the columns in P. Observe that P is simply the matrix whose columns are the basis vectors of S. This is true only because the original basis was the usual basis E.

(b) Find the change-of-basis matrix Q from the basis S to the basis E.

The definition of the change-of-basis matrix Q tells us to write each of the (usual) basis vectors in E as a linear combination of the basis elements of S. This yields

$$\begin{aligned} e_1 &= (1,0,0) = -2u_1 + 2u_2 - u_3 \\ e_2 &= (0,1,0) = -2u_1 + u_2 \\ e_3 &= (0,0,1) = 3u_1 - 2u_2 + u_3 \end{aligned} \qquad \text{and hence,} \qquad Q = \begin{bmatrix} -2 & -2 & 3 \\ 2 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix}$$

We emphasize that to find Q, we need to solve three 3×3 systems of linear equations—one 3×3 system for each of e_1, e_2, e_3.

Alternatively, we can find $Q = P^{-1}$ by forming the matrix $M = [P, I]$ and row reducing M to row canonical form:

$$M = \begin{bmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 1 & 2 & 2 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -2 & -2 & 3 \\ 0 & 1 & 0 & 2 & 1 & -2 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{bmatrix} = [I, P^{-1}]$$

thus,

$$Q = P^{-1} = \begin{bmatrix} -2 & -2 & 3 \\ 2 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix}$$

(Here we have used the fact that Q is the inverse of P.)

The result in Example 6.6(a) is true in general. We state this result formally, because it occurs often.

PROPOSITION 6.5: The change-of-basis matrix from the usual basis E of K^n to any basis S of K^n is the matrix P whose columns are, respectively, the basis vectors of S.

THEOREM 6.6: Let P be the change-of-basis matrix from a basis S to a basis S' in a vector space V. Then, for any vector $v \in V$, we have

$$P[v]_{S'} = [v]_S \qquad \text{and hence,} \qquad P^{-1}[v]_S = [v]_{S'}$$

Namely, if we multiply the coordinates of v in the original basis S by P^{-1}, we get the coordinates of v in the new basis S'.

Remark 1: Although P is called the change-of-basis matrix from the old basis S to the new basis S', we emphasize that P^{-1} transforms the coordinates of v in the original basis S into the coordinates of v in the new basis S'.

Remark 2: Because of the above theorem, many texts call $Q = P^{-1}$, not P, the transition matrix from the old basis S to the new basis S'. Some texts also refer to Q as the *change-of-coordinates* matrix.

We now give the proof of the above theorem for the special case that $\dim V = 3$. Suppose P is the change-of-basis matrix from the basis $S = \{u_1, u_2, u_3\}$ to the basis $S' = \{v_1, v_2, v_3\}$; say,

$$\begin{aligned} v_1 &= a_1u_1 + a_2u_2 + a_3a_3 \\ v_2 &= b_1u_1 + b_2u_2 + b_3u_3 \\ v_3 &= c_1u_1 + c_2u_2 + c_3u_3 \end{aligned} \qquad \text{and hence,} \qquad P = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix}$$

Now suppose $v \in V$ and, say, $v = k_1v_1 + k_2v_2 + k_3v_3$. Then, substituting for v_1, v_2, v_3 from above, we obtain

$$\begin{aligned} v &= k_1(a_1u_1 + a_2u_2 + a_3u_3) + k_2(b_1u_1 + b_2u_2 + b_3u_3) + k_3(c_1u_1 + c_2u_2 + c_3u_3) \\ &= (a_1k_1 + b_1k_2 + c_1k_3)u_1 + (a_2k_1 + b_2k_2 + c_2k_3)u_2 + (a_3k_1 + b_3k_2 + c_3k_3)u_3 \end{aligned}$$

Thus,

$$[v]_{S'} = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} \qquad \text{and} \qquad [v]_S = \begin{bmatrix} a_1k_1 + b_1k_2 + c_1k_3 \\ a_2k_1 + b_2k_2 + c_2k_3 \\ a_3k_1 + b_3k_2 + c_3k_3 \end{bmatrix}$$

Accordingly,

$$P[v]_{S'} = \begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} a_1k_1 + b_1k_2 + c_1k_3 \\ a_2k_1 + b_2k_2 + c_2k_3 \\ a_3k_1 + b_3k_2 + c_3k_3 \end{bmatrix} = [v]_S$$

Finally, multiplying the equation $[v]_S = P[v]_{S'}$, by P^{-1}, we get

$$P^{-1}[v]_S = P^{-1}P[v]_{S'} = I[v]_{S'} = [v]_{S'}$$

THEOREM 6.7: Let P be the change-of-basis matrix from a basis S to a basis S' in a vector space V. Then, for any linear operator T on V,

$$[T]_{S'} = P^{-1}[T]_S P$$

That is, if A and B are the matrix representations of T relative, respectively, to S and S', then

$$B = P^{-1}AP$$

EXAMPLE 6.7 Consider the following two bases of $\mathbf{R}^3$:

$$E = \{e_1, e_2, e_3\} = \{(1,0,0), \quad (0,1,0), \quad (0,0,1)\}$$

and

$$S = \{u_1, u_2, u_3\} = \{(1,0,1), \quad (2,1,2), \quad (1,2,2)\}$$

The change-of-basis matrix P from E to S and its inverse P^{-1} were obtained in Example 6.6.

(a) Write $v = (1,3,5)$ as a linear combination of u_1, u_2, u_3, or, equivalently, find $[v]_S$.
One way to do this is to directly solve the vector equation $v = xu_1 + yu_2 + zu_3$; that is,

$$\begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} = x\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + y\begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix} + z\begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \qquad \text{or} \qquad \begin{aligned} x + 2y + z &= 1 \\ y + 2z &= 3 \\ x + 2y + 2z &= 5 \end{aligned}$$

The solution is $x = 7, \quad y = -5, \quad z = 4, \quad$ so $v = 7u_1 - 5u_2 + 4u_3$.

On the other hand, we know that $[v]_E = [1,3,5]^T$, because E is the usual basis, and we already know P^{-1}. Therefore, by Theorem 6.6,

$$[v]_S = P^{-1}[v]_E = \begin{bmatrix} -2 & -2 & 3 \\ 2 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 7 \\ -5 \\ 4 \end{bmatrix}$$

Thus, again, $v = 7u_1 - 5u_2 + 4u_3$.

(b) Let $A = \begin{bmatrix} 1 & 3 & -2 \\ 2 & -4 & 1 \\ 3 & -1 & 2 \end{bmatrix}$, which may be viewed as a linear operator on $\mathbf{R}^3$. Find the matrix B that represents A relative to the basis S.

The definition of the matrix representation of A relative to the basis S tells us to write each of $A(u_1)$, $A(u_2)$, $A(u_3)$ as a linear combination of the basis vectors u_1, u_2, u_3 of S. This yields

$$\begin{aligned} A(u_1) &= (-1,3,5) = 11u_1 - 5u_2 + 6u_3 \\ A(u_2) &= (1,2,9) \quad = 21u_1 - 14u_2 + 8u_3 \\ A(u_3) &= (3,-4,5) = 17u_1 - 8e_2 + 2u_3 \end{aligned} \qquad \text{and hence,} \quad B = \begin{bmatrix} 11 & 21 & 17 \\ -5 & -14 & -8 \\ 6 & 8 & 2 \end{bmatrix}$$

We emphasize that to find B, we need to solve three 3×3 systems of linear equations—one 3×3 system for each of $A(u_1)$, $A(u_2)$, $A(u_3)$.

On the other hand, because we know P and P^{-1}, we can use Theorem 6.7. That is,

$$B = P^{-1}AP = \begin{bmatrix} -2 & -2 & 3 \\ 2 & 1 & -2 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & -2 \\ 2 & -4 & 1 \\ 3 & -1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 21 & 17 \\ -5 & -14 & -8 \\ 6 & 8 & 2 \end{bmatrix}$$

This, as expected, gives the same result.

Reg no-------------

(17MMU501A)

KARPAGAM ACADEMY OF HIGHER EDUCATION
Coimbatore-21
DEPARTMENT OF MATHEMATICS
Fifth Semester
I Internal Test – July 2018
Ring Theory and Linear Algebra I

Date: -07-2019 **Time: 2 Hours**

Class: III-B. Sc. Mathematics **Maximum Marks:50**

PART-A(20X1=20 Marks)

Answer all the Questions:

1. Every subgroup of Z is _________ of Z.
   (a) right ideal (b) left ideal (c) ideal (d) both (a) and (b)
2. If I is an ideal R then I is ________ of R.
   (a) ring (b) integral domain (c) sub ring (d) unique ideal
3. Which of the following is/are field?
   (a) Z (b) Q, R, C (c) Z_p (d) both (b) and (c)
4. The number of ideals of $Z_8 \times Z_{30}$ _________
   (a) 30 (b) 38 (c) 32 (d) 36
5. If R is commutative ring with identity then every maximal ideal of R is ________
   (a) Ideal(b) minimal ideal (c) prime ideal (d) sub ring
6. Which of the following is not true?
   (a) 2Z is prime ideal of Z (b) 5Z is prime ideal of Z
   (b) m > 1 then is prime ideal of Z
   (d) m > 1 then is not prime ideal of Z
7. A characteristic of ring (R, +, .) is _________
   (a) Positive integer (b) negative integer
   (c) order of a ring (d) least positive integer
8. If f : $Z_{20} \to Z_{20}$ then the number of ring homomorphism is _______
   (a) 5 (b) 4 (c) 0 (d) 1
9. Which of the following is Boolean ring _______
   (a) Q (b) R (c) (P(S), ∪,∩) **(d) (P(S), Δ,∩)**
10. A ring R is said to be commutative if _________
    (a) **ab = ba** (b) ab $\neq ba$ (c) $a^2 = b^2$ (d) $a^2 \neq b^2$
11. A commutative skew field is called _________
    (a) Sub ring (b) ring (c) integral domain **(d) field**
12. Any _________ integral domain is a field
    (a) infinite **(b) finite** (c) skew (d) non skew
13. A homomorphism of a ring into its self is called a _________
    (a) monomorphism (b) epimrphism
    (c) endomorphism (d) isomorphism
14. The only idempotent element of an integral domain are_____
    (a) 0 and prime **(b) 0 and 1** (c) primes (d) units
15. R is a sub ring of __________
    (a) Q (b) Z **(c) C** (d) N
16. The number of unit in the ring (Z,+,.) is _______
    (a) **2** (b) 1 (c) 3 (d) 4
17. The rings {0}and R are sub ring of the any ring R.{0} is called _____sub ring of R
    (a) infinite (b) singleton **(c) trivial** (d) Non trivial
18. The ring of Gaussian integer Z [i] = {a+ bi \ a, b ∈ Z} is________
    (a) Ring with zero divisor **(b) an integral domain**
    (c) Not an integral domain (d) both (a) and (b)
19. A ring nZ is a ________
    (a) **Ideal** (b) right ideal (c) left ideal (d) maximal ideal
20. The characteristic of Z_n is __
    (a) 0 **(b) n** (c) 1 (d) 2

PART-B (3X2=6 Marks)

Answer all the Questions:

21. Define Characteristic of a ring R.
22. Write an example of right ideal but left ideal.
23. Define Kernel of homomorphism.

PART-C (3X8=24 Marks)

Answer all the Questions:

24. (a) Prove that Z_n is an integral domain if and only if n is prime.

(OR)

(b) Prove that if R is a ring with identity then set of all units in R is a group under multiplication.

25. (a) Prove that any field is an integral domain. Also discuss for the converse part of the statement.

(OR)

(a) Prove that if R is a commutative ring with identity then an ideal M of R is maximal if and only if R/M is a field.

26. (a) Prove that the fundamental theorem of homomorphism.

(OR)

(b) Prove that if R is a commutative ring with identity then every maximal ideal is a prime ideal.

Reg no-------------

(17MMU501A)

KARPAGAM ACADEMY OF HIGHER EDUCATION

Coimbatore-21

DEPARTMENT OF MATHEMATICS

Fifth Semester

II Internal Test – July 2018

Ring Theory and Linear Algebra I

Date: -08-2019 Time: 2 Hours

Class: III-B. Sc. Mathematics Maximum Marks:50

PART-A(20X1=20 Marks)

Answer all the Questions:

1. Number of units in R is ___________
(a) finite (b) countable (c) infinite (d) uncountable
2. The set of all units in a ring R is _________ under multiplication
(a) ring (b) group
(c) both a and b (d) neither a nor b
3. Field is _________
(a) commutative (b) skew field
(c) neither a nor b (d) both a and b
4. The set of all matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ where $a, b \in Q\ is$ ___________
(a) commutative (b) with unity
(c) neither a nor b (d) both a and b
5. Which of the following is a field?
(a) Z (b) nZ (c)n+Z (d) Q
6. Number of identity elements exists in a ring is _____________
(a) 0 (b) 2 (c) 3 (d) 1
7. The set of all units in a ring R is not a group under ______________
(a) addition (b) multiplication
(c) both a and b (d) neither a nor b
8. Skew Field is also called as ______________
(a) integral domain (b) division ring
(c) neither a nor b (d) both a and b
9. The set of complex number C is ___________
(a) integral domain (b) field
(c) neither a nor b (d) both a and b
10. Which of the following is a field?
(a) Z (b) nZ (c) n+Z (d) R
11. Number of identity elements exists in a ring of integers is ______
(a) 0 (b) 2 (c) 3 (d) 1
12. 1 and -1 are the only units of _________
(a) Z (b) nZ (c) n+Z (d) R
13. Number of binary operations involved in vector space is ___________
(a) 0 (b) 1 (c) 2 (d) 2^2
14. Z_n is a ____________
(a) commutative ring (b) ring with unity
(c) both a and b (d) neither a nor b
15. $M_2(Z)$ is a _______________
(a) non commutative ring (b) ring with unity
(c) both a and b (d) neither a nor b
16. Which one of the following is not true_________
(a) set of all polynomial over F[x] (b) C is vector space over R
(c) R is vector space over R (d) R is vector space over C
17. The value of $(\alpha + \beta)(v)$ is ________
(a) vector (b) Scalar (c) both (d) neither nor
18. Dimension of any two basis in a vector space is_______
(a) Same (b) different (c) twice (d) not related
19. Dimension of a polynomial with degree n is _______
(a) n (b) n+1 (c) n-1 (d) 2n
20. The dimension of $m \times n$ matrices set is ______
(a) m+n (b) m-n (d) mn (d) m or n

PART-B (3X2=6 Marks)

Answer all the Questions:

21. Define a basis.
22. Define epimorphism.
23. Define linear span.

PART-C (3X8=24 Marks)

Answer all the Questions:

24. (a) State and prove first theorem isomorphism of rings.

(OR)

(b) Let V be vector space over a field F. Prove that a non-empty subset W of V is a subspace if and only if $u, v \in W$ and $\alpha, \beta \in F \Rightarrow \alpha u + \beta v \in W$

25. (a) Let H be a nonempty subset of a vector space V. Then prove that H is a subspace of V if and only if H is closed under addition and scalar multiplication.

(OR)

(b) Prove that the field of quotients F of an integral domain D is the smallest field containing D

26. (a) Let $S = \{v_1, v_2, \dots, v_n\}$ be a linearly independent set of vectors in a vector space V over a field $\mathbb{F}$ then prove $L(S)$ can be uniquely written in the form $\alpha_1 v_1 + \alpha_1 v_2 + \cdots + \alpha_n v_n$, where $\alpha_i \in \mathbb{F}$.

(OR)

(b) Let $f: \mathbb{Z} \to \mathbb{Z}_n$ be defined by $f(x) = r$ if $x = nq + r$, $0 \le r < n$. Prove that f is a homomorphism

Reg no-------------

(17MMU501A)

KARPAGAM ACADEMY OF HIGHER EDUCATION
Coimbatore-21
DEPARTMENT OF MATHEMATICS
Fifth Semester
III Internal Test – Oct'19
Ring Theory and Linear Algebra I

Date: -10-2019 **Time: 2 Hours**

Class: III-B. Sc. Mathematics **Maximum Marks:50**

PART-A(20X1=20 Marks)

Answer all the Questions:

1. Dimension of any two basis in a vector space is_______
   (a) Same (b) different (c) twice (d) not related
2. If T is a linear transformation , then T(0)=…………
   (a) 0 (b) 1 (c) 2 (d) 3
3. Let V& W be vector spaces over the field F. A linear transformation from V into W is a function T from V into W such that T(cu+v)=…………. for all u,v in V and all scalars c in F.
   (a) T(u)+T(v) (b) cT(u)+cT(v) (c) T(u)+cT(v) (d) cT(u)+T(v)
4. Every …………….. transformation is a linear transformation.
   (a) matrix (b) row (c) column (d) unit
5. The set of all vector space-homomorphisms of V into itself -------
   (a) Hom(V,W) (b) Hom(W,V) (c) Hom(V,V) (d) Hom(W,W)
6. A linear transformation on V,over F is an element of -----------
   (a) $A_F(W)$ (b) $B_F(V)$ (c) $A_F(V)$ (d) $W_F(V)$
7. An element T in A(V) is called -------------- if there exists an S in A(V) such that TS =1.
   (a) both invertible (b) right-invertible (c) right-invertible (d) invertible
8. The ----------T in A(V) is said to be unitary if (uT,vT)=(u,v) for all u,v in V
   (a) normal transformation (b) linear transformation (c) unitary (d) Nilpotent transformation
9. If V is finite dimensional and ------------ there is an SÎA(V) such that E=TS ¹0 is an idempotent
   (a) T>0 (b) T=0 (c) T $\neq$0 (d) T<0
10. Dimension of a polynomial with degree n is _______
    (a) n (b) n+1 (c) n-1 (d) 2n
11. The ------------- W of V is invariant under T in A(V) if WT contained W.
    (a) subspace (b) space (c) field (d) sub field
12. The element λin F is a characteristic root of T in A(V) if and only if for some ------- in V, vT=λv.
    (a) λ=0 (b) $\lambda \neq$0 (c) v=0 (d) v$\neq$0
13. The Hermitian ----------------- T is non negative if and only if its characterstic roots are non negative.
    (a) normal transformation (b) linear transformation (c) unitary (d) Nilpotent transformation
14. Any subset of a lineary independent set is …………….....
    (a) linearly dependent (b) linearly independent (c) linear (d) non linear
15. Any set which contains a lineary dependent set is …………….....
    (a) linearly dependent (b) linearly independent (c) linear (d) non linear

16. The subset consisting of the……………. vector alone is a subspace of V, called zero subspace of V.
    (a) zero (b) unit (c) unit (d) infinite
17. A product of invertible ……………. is invertible
    (a) matrices (b) functions (c) vectors (d) equations
18. A polynomial with coefficients which are complex numbers has all its roots in the -------------
    (a) real field (b) rational field
    (c) complex field (d) irrational field
19. If T ÎA(V) isHermitian then all its characteristic roots are --------
    (a) real (b) complex (c) rational (d) irrational
20. The dimension of $m \times n$ matrices set is ______
    (a) m+n (b) m-n (d) mn (d) m or n

PART-B (3X2=6 Marks)

Answer all the Questions:

21. Define rank of a linear transformation.
22. Define isomorphism.
23. Define direct sum of two sub spaces.

PART-C (3X8=24 Marks)

Answer all the Questions:

24. a) Let $S = \{v_1, v_2, \dots, v_n\}$ be a linearly independent set of vectors in a vector space V over a field $\mathbb{F}$ then prove $L(S)$can be uniquelywritten in the form $\alpha_1 v_1 + \alpha_1 v_2 + \cdots + \alpha_n v_n$, where $\alpha_i \in \mathbb{F}$.

(OR)

b) State and prove basis theorem.

25. a) State and prove fundamental theorem of homomorphism of linear transformations

(OR)

b) Let V and W be two vector spaces. Suppose $T : V \to W$ is a linear transformation. Then prove the following

i) $T(0) = 0$.

ii) $T(-v) = -T(v)$ for all $v \in V$.

28. a) State and prove fundamental theorem of homomorphism of linear transformations

(OR)

b) State and prove rank theorem